MISSION AREA INITIAL CAPABILITIES DOCUMENT (MA ICD)

GLOBAL INFORMATION GRID (GIG)

JROCM 202-02
22 November 2002

[JROCM and date listed refer to the latest JROC Approval of the GIG Capabilities Requirement Document (CRD). This MA ICD is a cut-and-paste conversion of the GIG CRD to MA ICD directed by JROCM 095-04 of 14 June 2004]

MA ICD Executive Agent

Commander
U.S. Joint Forces Command
Attn: C4 Plans, Policy and Projects Division (J68)
1562 Mitscher Avenue
Norfolk, VA 23551-2488
DSN: 836-5871; COM: 757-836-5871
NIPRNET Email: J68actions@jfcom.mil
SIPRNET Email: J68actions@hq.jfcom.smil.mil

Document Revision and Change Log

All changes commented on are relative to changes after Capstone Requirements Document (CRD) Global Information Grid (GIG) JROCM 134-01 30 August 2002.

Version	Change Date	Remarks	Paragraphs Affected
MA ICD	14 Aug 04	Chapter headings and appendices changed per JROCM 095-04 14 June 2004 for MA ICD conversion. Sample GIG CRD Crosswalk (Appendix F) chapter headings changed to reflect new MA ICD chapter headings.	All chapter headings and appendices. Appendix F.
MA ICD	14 Aug 04	Paragraph numbering changed from GIG CRD numbering to match new chapter headings of MA ICD	Various throughout document
MA ICD	14 Aug 04	All references to CRD changed to MA ICD	Various throughout document
MA ICD	14 Aug 04	Net Readiness support pointer to Appendix H	Paragraph IV.C
MA ICD	14 Aug 04	NR KPP support information	Appendix H
MA ICD	14 Aug 04	GIG MA ICD supercedes IDM CRD	Paragraph I.A.5
MA ICD	14 Aug 04	All references to NIMA changed to NGA	Various throughout document
MA ICD	14 Aug 04	All references to JTA changed to JTA/DISR	Various throughout document
MA ICD	14 Aug 04	Integrated Architecture Products included as separate appendix	Appendix B
MA ICD	14 Aug 04	Preface added	Preface
MA ICD	14 Aug 04	Table D-2 GIG IER Matrix shortened for brevity	Table D-2
MA ICD	14 Aug 04	Appendix A expanded to include information available at USJFCOM Joint Digital Library web site.	Appendix A

Table of Contents

Preface

On 14 Jun 2004, Joint Requirements Oversight Council Memorandum (JROCM) 095-04 was issued requiring the conversion of existing Capstone Requirements Documents (CRD) to Mission Area Initial Capabilities Documents (MA ICD). One of the objectives of Joint Capabilities and Development Information System (JCIDS) process is to eliminate reliance on system-oriented CRDs as a way of enforcing standards and ensuring interoperability to deliver capabilities in key mission areas. Progress continues towards this objective by converting all JCIDS-approved CRDs to MA ICDs. MA ICDs are the next step in ensuring capabilities that contribute to specific mission areas comply with the standards and Key Performance Parameters (KPP) necessary for the successful accomplishment of that mission.

While the JROCM guidance for this stage of the CRD to MA ICD conversion was to conduct a “cut and paste,” it seemed reasonable and appropriate to make textual changes to correct any identified outdated information. All textual changes have been documented on the Change Page and it is affirmed that none of these changes have affected the basic intent or purpose of the JROC approved GIG CRD.

Any questions may be directed to the POCs of this document:

Mr. Robert B. Powers
757-836-9536 (COMM)
836-9536 (DSN)
robert.powers@jfcom.mil

Mr. Jose Longoria
757 836 7269 (COMM)
836 7269 (DSN)
jose.longoria@jfcom.mil

CHAPTER I JOINT FUNCTIONAL CONCEPT

A. Introduction

1. GIG Concept. The concept of a "Global Information Grid" (GIG) was born out of concerns regarding interoperability and end-to-end integration of automated information systems. Issues such as streamlined management and the improvement of information infrastructure investment have also contributed to the heightened interest in a GIG. However, the real demand for a GIG has been driven by the requirement for information superiority and decision superiority to achieve full spectrum dominance, as expressed in Joint Vision 2020 (JV 2020). JV 2020 also highlights the importance of a network-centric warfare (NCW) environment, enabled by the GIG by means of dramatically improved information sharing through the robust networking of warfighting forces. As depicted in Figure 1, the GIG provides the enabling foundation for NCW[1], information superiority, decision superiority, and ultimately full spectrum dominance. The information advantage gained through the use of NCW allows a warfighting force to achieve dramatically improved information positions, in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power. The ability to achieve shared situational awareness and knowledge among all elements of a joint force, in conjunction with allied and coalition partners, is increasingly viewed as a cornerstone of transformation to achieve future warfighting capabilities. The success of the GIG will depend in large part on how well it helps achieve fully interoperable forces by connecting today's islands of interoperability to allow force-wide information sharing.

[1] An in-depth treatment of NCW Is provided in the book *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised), by David S. Alberts, John J. Garstka and Frederick P. Stein, C4ISR Cooperative Research Program (CCRP), August 1999.

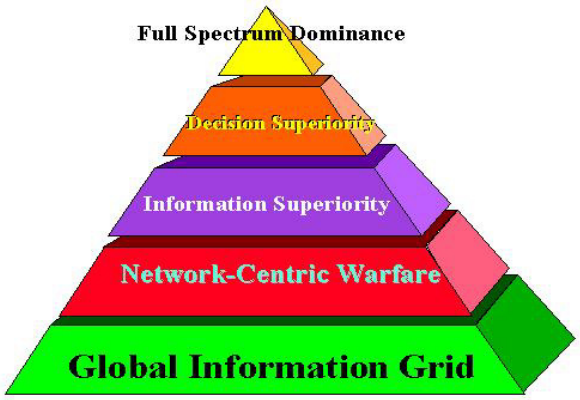


Figure 1. GIG as an Enabling Foundation

2. The GIG Vision. In the pamphlet entitled "Enabling the Joint Vision" (accessible on the Web at http://www.dtic.mil/jcs/j6/enablingjv.pdf) the Chairman of the Joint Chiefs of Staff envisions the GIG as:
   - A single secure grid providing seamless end-to-end capabilities to all warfighting, national security, and support users
   - Supporting Department of Defense (DoD) and Intelligence Community (IC) requirements from peace time business support through all levels of conflict
   - Joint, high capacity netted operations
   - Fused with weapons systems
   - Supporting strategic, operational, tactical, and base/post/camp/station
   - Plug and Play interoperability
     - Guaranteed for US and allied
     - Connectivity for coalition users
   - Tactical and functional fusion a reality
   - Information/bandwidth on demand
   - Defense in depth against all threats

3. GIG Definition. A DoD Chief Information Officer (CIO) memorandum, dated 22 September 1999, established the definition of the GIG, which subsequently was revised on 2 May 2001, by agreement among the DoD CIO, the Under Secretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L), and the Joint Staff/J6. The GIG is defined as follows:

   a. Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and

support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

b. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:
   - Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
   - Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
   - Processes data or information for use by other equipment, software, and services.

c. Non-GIG Information Technology (IT) – Stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

4. Background. The task of preparing the GIG Capstone Requirements Document (CRD) was assigned to the United States Joint Forces Command (USJFCOM) by the Joint Chiefs of Staff (JCS) Joint Requirements Oversight Council (JROC) under the sponsorship of the Joint Staff Command, Control, Communications and Computer (C4) Systems Directorate (J6) and the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD [C3I]). JROC Memorandum 135-99 (JROCM 135-99) of 23 November 1999 outlined the task for the development of this CRD. This document is the culmination of multiple strategy meetings and coordination initiatives that have occurred since 23 November 1999. The CRD development process was assisted by representatives from other Commanders in Chief (CINCs), Services, and Agencies, who participated in the GIG requirements development conference held 4 – 6 April 2000, and provided input during subsequent document review and comment phases. On 14 Jun 2004, Joint Requirements Oversight Council Memorandum (JROCM) 095-04 was issued requiring the conversion of existing Capstone Requirements Documents (CRD) to Mission Area Initial Capabilities Documents (MA ICD).

5. Purpose. The purpose of this MA ICD is to describe the overarching information capabilities required for a globally interconnected, end-to-end, interoperable, secured system of systems that will support the National Command Authorities (NCA), warfighters, DoD personnel, IC, policy makers, and non-DoD users at all

levels involved in both military and nonmilitary operations. The GIG MA ICD supersedes the Information Dissemination Management (IDM) CRD.

6. Content. The organization and content of this MA ICD are in compliance with JROCM 095-04 dated 14 June 2004. However, as allowed by paragraph 2 of the JROCM, some flexibility was exercised in the format conversion to allow for the variance in the GIG CRD, as written to the requirements of CJCSI 3170.01B, and the format specified by JROCM 095-04. This version of the GIG MA ICD complies with, and continues to support the GIG guiding documentation listed below:
   - Chairman, Joint Chiefs of Staff's GIG Vision (see paragraph I.A.2 above)
   - OASD (C3I) NCOW Reference Model
   - OASD (C3I) GIG Architecture
   - DoD GIG definition (see paragraph I.A.3 above).
7. Scope. The GIG is a system of systems that provides a set of value-added functions operating in a global context to provide processing, storage, and transport of information; human-GIG interaction; network management; information dissemination management; and information assurance. These functions are fully interrelated, integrated, and interoperable with one another in order to achieve overall interoperability across the GIG. As a result, the GIG is an information environment comprised of interoperable computing and communication components.
8. Applicability. The capability requirements and the Key Performance Parameters (KPPs) (including the information exchange requirements and the interoperability KPP) outlined in this MA ICD provide direction to all DoD and IC components in developing Capability Development Documents (CDDs) and Capability Production Documents (CPDs). For new systems and for upgrading legacy systems. This MA ICD also guides future IT investments to ensure interoperability. All JCIDS directed capability documents that are associated with GIG systems, regardless of acquisition category (ACAT), must show compliance with this MA ICD, as appropriate and necessary to fulfill a system's operational purpose(s)/mission(s).

B. Mission Area Description

1. Summary of Mission Need**.** A formal MNS for the GIG does not exist. However, in a 1998 memorandum to the Joint Staff J6, the Director of the Defense Information Systems Agency (DISA) articulated the need for a "Defense Information Infrastructure Capstone Requirements Document." After further study and consideration by the Joint Staff, OASD(C3I), and others within DoD, this seminal idea was expanded upon and re-characterized in terms of scope and intent into a concept, which by 1999 was officially known as the Global Information Grid (GIG). The need for the GIG also has been documented in a number of major reference publications, such as *Joint Publication 6-0* and *JV 2020,* as well as various published MNSs, ORDs, and MA ICDs (e.g., Defense Information Systems Network CRD, Global Broadcast Service ORD, Information

Dissemination Management CRD, Joint Tactical Radio System ORD, Global Combat Support System MA ICD, Theater Air and Missile Defense CRD, Warfighter Information Network – Tactical ORD, Joint Network Management System ORD, and Combat Identification CRD).

2. The GIG is a key enabler of network-centric warfare and is essential for information and decision superiority. It will enable Command, Control, Communications, Computers and Intelligence (C4I) integration of joint forces, improve interoperability of systems, and increase optimization of bandwidth capacity thereby dramatically improving the warfighting capabilities of joint forces across the full spectrum of conflict. The GIG will enhance operational capabilities while providing a common operational environment for conventional and nuclear command and control (C2), combat support, combat service support, intelligence, and business functions. In particular, the GIG will support:
   - Warfighters' ability to operate with reduced forces at high operational tempos where dynamic planning and redirection of assets is the norm.
   - Delivery of information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets to joint commanders, their forces, and the NCA within specified time frames.
   - Warfighters' ability to obtain and use combat and administrative support information from national, allied, coalition, and other widely dispersed assets.
   - Collection, processing, storage, distribution, and display of information horizontally and vertically throughout organizational structures across the battlespace.
   - Rapid and seamless flow and exchange of information around the globe to enable collaborative mission planning and execution from widely dispersed locations and at different levels (to include strategic, operational, tactical, and business).
   - Timely, assured connectivity and information availability for decision makers and their advisors to support effective decision making.
   - Integrated, survivable, and enduring communications for the NCA, Integrated Tactical Warning and Attack Assessment (ITW/AA), and strategic forces.
3. Related documents. There are currently no approved MA ICDs or ORDs, which pertain exclusively to the required capabilities described in this MA ICD, except for the [obsolete] Information Dissemination Management (IDM) CRD (dated 8 May 2001) which focuses on the IDM function. However, there are numerous proposed, draft, and current requirements documents (such as those cited in paragraph B.1 above, and the GIG Enterprise Services CDD currently being drafted) that address GIG functionality in some fashion.
4. Possible implications for changes to joint doctrine. All doctrinal publications that refer either to information management or to any of the functions of the GIG (see section C below) may have to be updated in accordance with the capabilities outlined in this document.

C. GIG Functions

The functions that support and characterize the information flow and exchange throughout the GIG are organized and defined as follows:

1. Computing
   - Process Function: A set of operations performed on well-defined inputs to produce a specified output. Computer-based processing is typically used for manipulating data, information, and/or knowledge into the desired form to support decision making and other GIG functions.
   - Store Function: The retention, organization, and disposition of data, information, and/or knowledge to facilitate information sharing and retrieval.
2. Communications
   - Transport Function: End-to-end movement of data, information, and/or knowledge between users and producers through other intermediate GIG entities.
3. Presentation
   - Human-GIG Interaction (HGI) Function: The input and output of information representations between human(s)-in-control and GIG entry point(s).
4. Network Operations

   Network Operations (NETOPS) is an organizational and procedural framework for integrating Network Management (NM), Information Dissemination Management (IDM) and Information Assurance (IA).
   - Network Management (NM) Function: The capability to monitor, control and ensure the visibility of the various networking and internetworking components.
   - Information Dissemination Management (IDM) Function: Capability achieved through the use of a Family of Applications, Processes, and Services (FoAPS) to provide awareness, access, and delivery of information by the most effective and efficient means in a manner consistent with a commander's policy. The IDM FoAPS concept requires that each IDM element be designed to be interoperable with other IDM elements as a condition of membership in the family. The IDM FoAPS will be the principal means for managing the dissemination and storage of information across the GIG. The IDM FoAPS will provide a set of information dissemination and storage management tools and standards that will enable:
     - Commanders to adjust information delivery priorities dynamically based on operational conditions and communications (bandwidth) availability
     - Commanders to make more efficient use of the allocated bandwidth
     - Information producers to advertise, publish, and distribute information to a widely dispersed, heterogeneous user community

- Information users to query information holdings and acquire needed information based on intelligent subscription to information products published on a recurring or situation-driven basis

- The IDM function includes the following services:
  - Awareness: Information awareness services allow warfighters and other DoD users of information to discover what information is available both inside and outside of their respective communities and to determine what information has changed.
  - Access: Information access services allow warfighters and other DoD users of information to state their information needs and access information without being aware of the details involved in the retrieval process.
  - Delivery: Information delivery services optimize the use of infrastructure resources required to provide the requested service and in accordance with the commander's policy in effect.
  - Support: IDM support services provide the necessary interfaces to other GIG functions (e.g., store, information assurance, network management, etc.) to enable information awareness, access, and delivery.
- Information Assurance (IA) Function: Information operations protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

D. Operational Suitability and Infrastructure Support

1. Operational suitability is the degree to which GIG-enabled[4] systems can be satisfactorily developed, fielded, deployed, operated, and sustained while meeting performance parameters and the users' needs. The following guidelines are provided to help in implementing the GIG:

   a. The GIG should be implemented in accordance with the standards included in the most current version of the DoD Information Technology Standards Registry (DISR) [formerly known as the DoD Joint Technical Architecture] unless waived in accordance with the waiver process described in DoDI 5000.2-R.

   b. Pursuant to Deputy Secretary of Defense Memorandum (control number U18556-03 dated 12 Nov 2003), all fielded C2, Combat Support and Intelligence Systems shall be GIG-enabled and compliant with the Common

[4] Any system that exchanges and/or disseminates information in the manner described in the GIG definition, and is in compliance with the capability requirements stated in the GIG MA ICD, as appropriate and necessary to fulfill the system's operational purpose(s)/mission(s), is considered to be GIG-enabled. This term is used similarly to the terms "Internet-enabled" and "Web-enabled."

Operating Environment (COE) (formerly known as Defense Information Infrastructure [DII] COE) compliant. Once the GIG Enterprise Services, Core Enterprise Services (GIG ES-CES) are mandated and a transition plan executed, then all GIG enabled systems shall be GIG ES-CES compliant.

c. GIG-enabled systems should be either standards-based or commercial-off-the-shelf (COTS) technologies that will:
   - Facilitate joint, allied, and coalition interoperability
   - Simplify integration
   - Reduce both long- and short-term costs

d. GIG-enabled systems should be scalable, affordable, sustainable, and extensible with respect to their functionality.

e. GIG-enabled systems should be designed to accommodate change and should facilitate the integration of future systems and technologies as they evolve. Moreover, procedural and architectural choices should be made that will facilitate the timely integration of technology without unacceptably degrading the security of the GIG.

f. GIG-enabled systems should be consistent with the current DoD, IC, and commercial efforts regarding data and metadata standardization.

g. The goal and expectation of proposed GIG-enabled systems should be to minimize additional manpower requirements.

h. The reliability, availability, survivability, and maintainability features of GIG-enabled systems should be designed to support all functions necessary to meet the requirements documented in Chapter IV, including the ability to recover from critical failures.

i. GIG-enabled systems should be fielded with an emphasis on reducing the complexity, time, and cost of training. User training concepts should incorporate embedded training capabilities to the maximum extent feasible. In addition to being cost effective, human-machine interface design should be consistent with the capabilities and limitations of operators and support personnel. Human-computer interface should also be designed to ensure quick and accurate information manipulation and assimilation. The utilization of existing installations and facilities for user training and support should be maximized.

j. Support functions and equipment should be consistent with operational requirements outlined in this MA ICD. Furthermore, software design should enhance interoperability and commonality within GIG-enabled systems.

k. GIG-enabled systems should be designed using an open systems approach and adhere to applicable standards within the Joint Technical Architecture (JTA/DISR).[5]

[5] Joint Technical Architecture (JTA) can be found at http://www-jta.itsi.disa.mil.

l. Bandwidth and throughput requirements along with implications to strategic, fixed, theater, and tactical architectures should be considered during the CDD/CPD and C4 Information Support Plan (ISP) development process.

m. National Geospatial-Intelligence Agency (NGA): United States Imagery and Geo-spatial Information Service (USIGS) standards should be used for the processing and display of imagery and geospatial data across the GIG.

n. GIG-enabled systems should be developed, tested, and deployed in a manner that is compliant with all appropriate treaties and international agreements.

o. GIG-enabled systems should be tested and certified for interoperability IAW Joint Interoperability Test Command (JITC) procedures.

p. Where applicable, GIG-enabled systems should enable users to operate from within the GIG to entities external to the GIG in a multilingual environment. This is essential to overcome the inherent language barriers common to multinational and coalition operations.

q. GIG capabilities may require a re-evaluation of existing security measures currently in place. However, GIG-enabled systems and associated applications, processes, and services should mitigate security risks and should meet all current security provisions articulated in appropriate DoD and IC policies, procedures, and instructions, including DoD 8500.aa, Information Assurance.

r. GIG-enabled systems should use standards-based rather than system-unique security mechanisms. Proprietary or unique security mechanisms should be considered only if commercial, standards-based security mechanisms prove to be inadequate or unavailable.

s. CDD/CPD writers should consider ongoing developments and evolving specifications in the following areas (as applicable):

- Joint Operational Architecture (JOA)
- Nuclear C2 System Technical Performance Criteria (NTPC)
- GIG Architecture
- Mission Information Management (MIM) Architecture

t. In accordance with DoDI 5000.2, CDD/CPD writers should develop time-phased requirements with associated objectives and thresholds (as appropriate).

u. A checklist is provided in Appendix F for CDD/CPD/MA ICD authors to use in completing a capability requirements crosswalk to ensure compliance with the GIG MA ICD as appropriate/applicable.

2. Use of Standards. Enforcement of IT and architecture standards is an essential element for achieving interoperability across the GIG. However, the use of standards alone is not sufficient to ensure interoperability among systems.

a. Compliance. GIG systems should be implemented in accordance with the latest versions of the *DoD JTA*/DISR unless waived in accordance with the waiver process described in DoDI 5000.2-R. Systems that are part of host nation and bilateral agreements should be checked for their ability to interface with the GIG.

b. Interoperability Testing and Certification. Interoperability testing and certification should be addressed as an integral part of the requirements generation process prior to production, fielding, and life cycle support, as required, of GIG systems regardless of ACAT level, in accordance with CJCSI 6212.01.

c. Technology Insertion. The GIG should apply open-system design strategies to enable the insertion of new and emerging technologies while maintaining interoperability with existing GIG systems and architectures. However, emerging technologies, for which standards do not exist, may be incorporated with an appropriate waiver to the JTA/DISR, only if they can integrate in a seamless and efficient manner (i.e., without compromising interoperability or GIG functionality requirements). Such JTA/DISR-waived technology insertions should be reviewed for feasibility of replacement with standards-based technology when appropriate.

d. Data Standards. All GIG systems should support standardized semantic tagging of data, unless it is not feasible to do so (such as may be the case with certain legacy systems). Both the syntax and semantics of GIG data and semantic tagging mechanisms should comply with applicable DoD standards. In cases where standards do not exist for a class of data, the developer should unambiguously define the syntax and semantics.

e. Net-Readiness. Because this document represents a conversion of the GIG CRD to a GIG Mission Area ICD, it is still considered a "legacy" Joint Requirements Document that, per CJCSI 6212.01C dated 20 November 2003, must continue to use the Interoperability KPP (I-KPP). However, also per direction of CJCSI 6212.01C, CDDs and CPDs initiated six months after the Instruction's publication date (on or after 21 May 2004) must include a Net-Ready Key Performance Parameter (NR-KPP) with associated metrics and performance measures, in lieu of the I-KPP. In light of this, Appendix H, “Net-Ready Key Performance Parameter (NR-KPP) Compliance Guidelines” is provided herein to assist CDD and CPD authors in preparing a NR-KPP that properly addresses interoperability within a GIG capabilities context. Appendix H offers specific guidance and assistance in understanding net-centric attributes and capabilities required to move into the net-centric environment in the GIG, and in determining and documenting NR-KPP compliance. The Appendix contains relevant material excerpted from Enclosures F through G of CJCSI 6212.01C; from Chapter 7 of the Defense Acquisition Guidebook, “Acquiring Information Technology and National Security Systems;” and from the OSD NII/DCIO Net-Centric Checklist. The latest version of the Defense Acquisition Guidebook can be found at **http://dod5000.dau.mil/** and the most current version of the Net-Centric

Checklist is located at the NII Document Archives site at **http://www.dod.mil/nii/doc/** (a listing of Net-Centric Attributes can also be found at this site).

CHAPTER II OPERATIONAL CONCEPT SUMMARY

A. GIG Operational Concept

1. The basic operational concept of the GIG is that warfighters and other authorized users in the DoD and IC, at any time and anywhere, can plug into the GIG and satisfy their validated user information requirements. From a logical perspective, the operational vision of the GIG is to facilitate interoperability among the fundamental building blocks/modules, i.e., the operational elements of the existing IT infrastructure. By integrating disparate systems and networks into a unified global system of systems, the GIG will empower warfighters with both information and decision superiority in every situation.
2. As a system of systems designed to foster integration, collaboration, and interoperability, the GIG is envisioned as a key enabler of information and decision superiority. It provides high quality, adaptive, and scalable information capabilities to meet, dynamically, the changing information needs of a warfighter.
3. The GIG will support DoD and IC information requirements and allow warfighters and other authorized users to process, store, transport, and use information regardless of technology, organization, or location. U.S. forces will have “plug and play” interoperability, while allied and coalition partners will be afforded connectivity on an as needed basis. The GIG will enable all warfighters to receive near real time , fused battlespace situational awareness. It will allow commanders and their staff at the Combatant Command, Joint Task Force (JTF), and Service Component levels to analyze data, anticipate requirements, focus on answers, and make real time decisions rather than relying on historical information from multiple stovepiped automated information systems applications. Finally, the GIG will provide commanders with the environment needed to support information flow and exchange to accomplish missions collaboratively, simultaneously, and interactively, resulting in more efficient and substantially reduced operational decision making times.
4. Figure 2 depicts a high-level operational view of the GIG. It shows the organization of the logical GIG functions and their interrelationships, which are internal to the GIG. Also included in the operational view are the entities (e.g. allied, coalition, non-DoD and other external) that reside in the environment external to the GIG. The GIG is required to interface with these external entities when engaged in the exchange and dissemination of information with them. From the perspective of those entities, the GIG is a virtual unified system of systems that interacts with them as a whole.

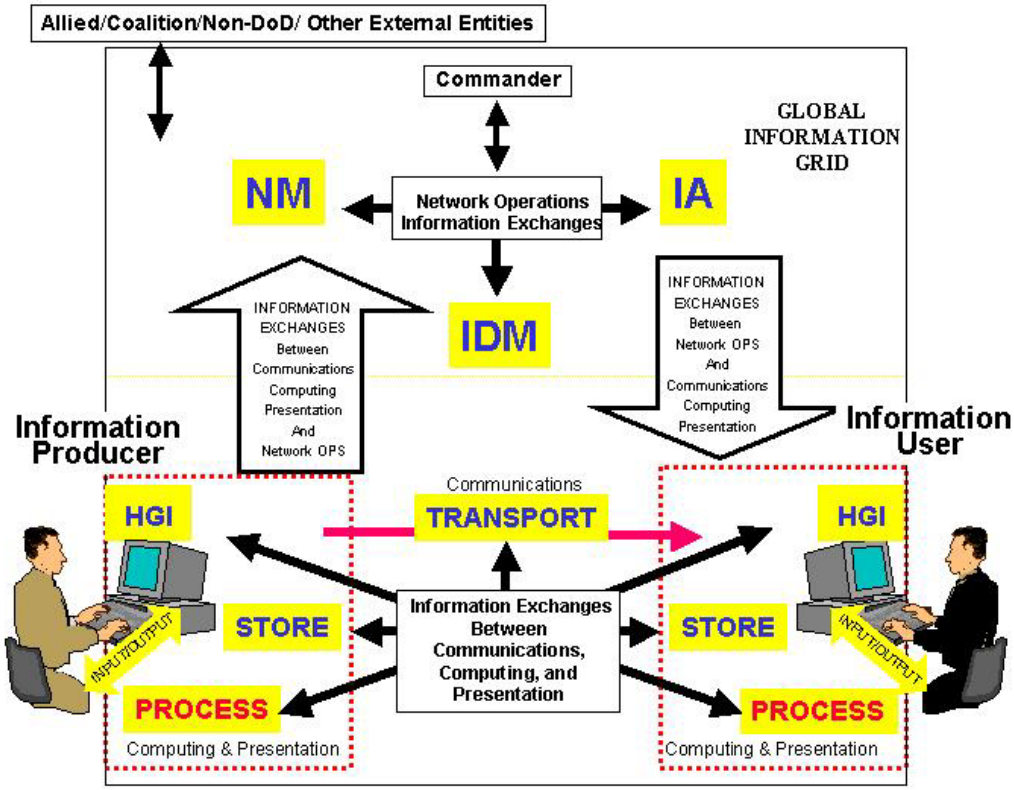


Figure 2. High-Level Operational View (OV-1)

5. The dynamic nature of information flowing across the GIG, and the time constraints within which information must often be delivered, require a new paradigm for characterizing and categorizing information. This new paradigm is based on the recognition that the first decision information users must make regarding a piece of information is whether it requires them to take immediate action. The IDM function of the GIG will drive the dissemination of extremely time-critical information to those users who need it by matching the time-critical information elements with specific users. For these users, the identified time-critical information elements are called "survival information" because they convey one of the following three basic factors:
   - information that requires the recipient to take immediate action to avoid danger or hostile action
   - information that is essential to enable the recipient to take immediate action to destroy, nullify, or defeat a hostile entity, weapon, or force
   - information that will prevent the recipient from causing fratricide
6. The concept of survival information can be described as follows:
   - It is a subset of the information required for battlespace situational awareness (SA). This implies that all survival information is relevant to SA. However, not all information used for SA can be considered as survival information.
   - It pertains to perceived threats in the area of operations that are geospatially related to the individual warfighter or the fighting platform. Hence it informs

about objects and events in the geospatial region around a warfighter that can cause destruction of life and property.

- It is of short duration and prompts either an immediate action or a decision from the recipient.
- Survival information is also dependent on the context determined by current mission, operating environment, and commander's intent.
- Survival information is generally predetermined by the user on the basis of perceived threats.
- It is unique and distinct to each individual, process, and fighting platform in the battlespace. This implies that the same information element can be treated as survival information for one warfighter and as "planning information" for another.
- It is required by individual warfighters and fighting platforms (to include systems and processes) in real time or near real time. For survival information, near real time latency cannot exceed a certain timeliness factor of "n" seconds (see Survival Information Dissemination KPP in Chapter IV.B.6.b.(25)) when the information is traveling from the exit point of B to F along the information delivery path as shown in Figure 3. In the path model, B is the first processor utilized that identifies an information element as survival information and designates the associated recipient(s). F is the final recipient (information user) of the processed survival information. It should be noted that the processing time at B is being excluded, whereas any processing beyond B is included in the specified timeframe.

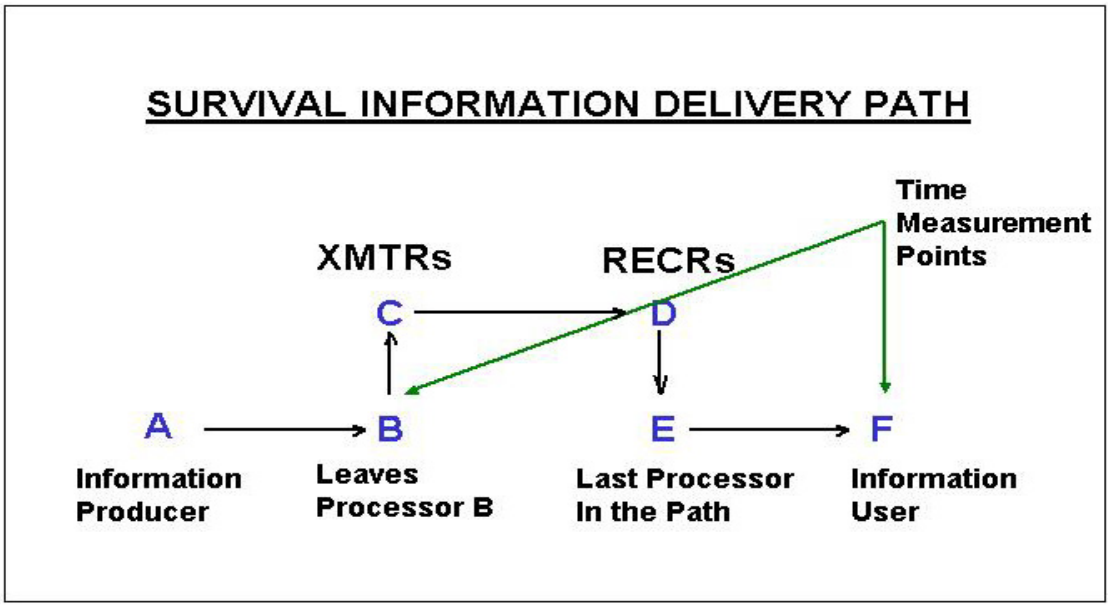


Figure 3. Information Path from Producer to User

7. The paradigm also addresses the requirements of the majority of users and information elements that do not meet the above described survival criteria. For

these users, information is characterized as planning information because, even though in some cases it can be time sensitive, it is used to support some action in the future (including the near future). While it is true that some planning information requires time-sensitive dissemination for some users, it still does not meet the life-threatening time-critical survival requirements. Although this MA ICD does not attempt to subcategorize planning information into various delivery timeliness groupings, it is fully understood and accepted that specific Service or system CDD/CPD requirements may require further definition and/or categorization of planning information into distinct levels. To this end, multiple levels of planning information delivery requirements may be specified within an CDD/CPD.

8. Even though some information may be very time sensitive, if it does not meet the survival criteria listed above, it will be characterized as planning information. Generally, planning information is not as time sensitive as survival information. It is usually used for determining a future course of action and deliverable within the time limits specified by a user. When requesting planning information, users typically will either rely on the best efforts of the delivery system or may choose to specify an upper limit for information delivery time. Depending on user needs, the specified time limit for planning information can range from several seconds to hours or days.

9. The concept of survival and planning information is depicted graphically in Figure 4, where the threat is an incoming Scud missile. There are two users who would need the information on the incoming Scud delivered as survival information in "n" seconds[3] or less. The Division Headquarters, as the probable target, needs to receive the information to prevent or reduce damage to itself from the impact of the Scud, and the Patriot Battery needs the information to engage the Scud and attempt to destroy it in flight. The third user shown in Figure 4, the afloat Battle Group, would need the same information delivered as planning information, so that it can take the Scud launch into account when planning future actions. Note that transmissions of survival information are typically short bursts, and require minimal processing by the recipient.

[3] See Chapter IV.B.5.b.(15) for Survival Information Dissemination KPP metrics.

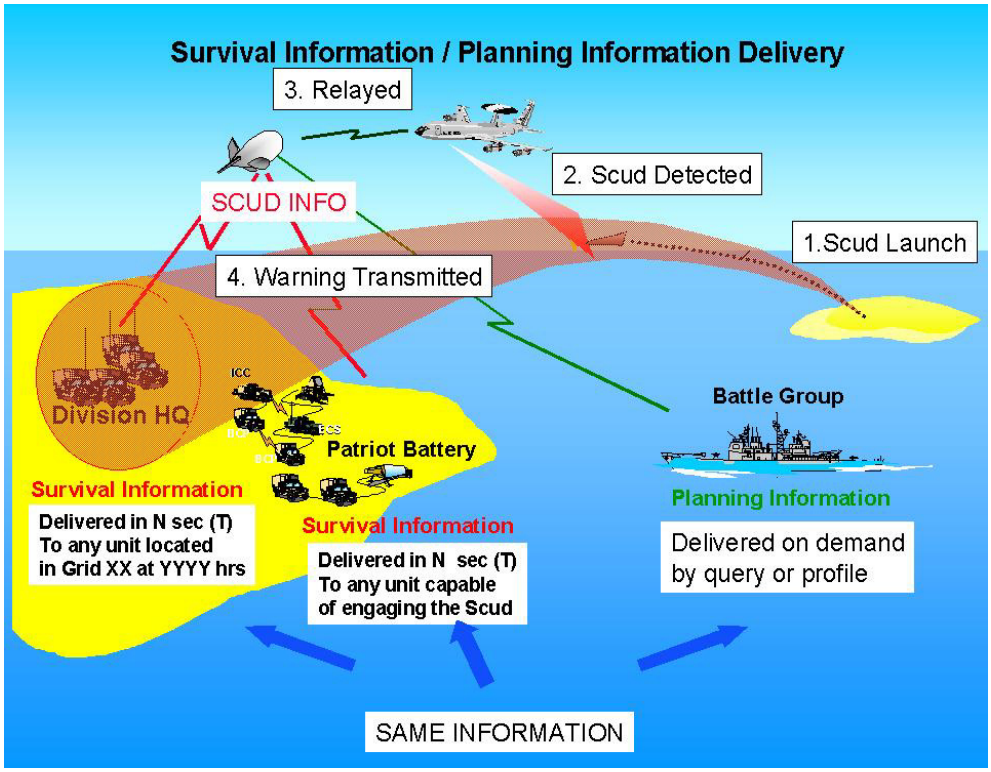


Figure 4. Survival / Planning Information Example

10. As shown in Figure 4, categorization of information as survival or planning will depend on the operational situation, including both the geographic location and operational mission of the information user. Therefore, it is the context that determines whether a particular information element meets the survival or planning criteria. Under predefined circumstances, certain information elements meeting the survival criteria for identified information users, and thus requiring real time delivery, must be disseminated to those users based on either an automatic response to a user profile or a manual response to a user query. In either case, once an information producer determines that information needed is of a survival nature, the information is then immediately disseminated. Such information elements requiring real time delivery to designated users are classified as survival information for those users. Non-time-critical information elements are classified as planning information. This classification is determined by the time needed for the recipient/information user to make a decision based on the received information. As is the case with survival information, information producers will disseminate planning information based on either an automatic response to a user profile or a manual response to a user query. While it is true that some planning information requires time-sensitive dissemination to some users, it still does not meet the life threatening time-critical survival requirement. As illustrated in Figure 4, it is also possible for the same information to be survival information for one user and planning information for another.

CHAPTER III CAPABILITY GAPS

A. General

1. Timely, relevant, consistent and accurate information is a fundamental requirement of the military decision making process. DoD and IC face many challenges meeting this basic requirement, to include the use of multiple information formats, non-interconnected communications systems, and the absence of a common cataloging scheme for indexing information. Furthermore, some currently fielded information systems may not support the robust, assured, and timely flow of accurate and relevant information needed to meet future joint warfighting needs. In addition, operational fragmentation and segregation of information by type, classification, command, and mission make it difficult to transport, store, and process essential information across/within the JTF. The information flow problems are especially critical with our allied and coalition partners.

2. Information needed by the military and the capabilities to provide that information are undergoing a revolutionary transformation. Global communications, data storage capacity, transmission speeds, information availability, and resulting bandwidth demands are all growing exponentially. However, our need for timely and precise information also continues to grow at a tremendous rate. Improvements in information technology and the evolution of commercial and IT standards have outpaced our processes and tools for managing information and its dissemination. Search and retrieval capabilities are hampered by the lack of a common data standard. Finding and accessing specific information can be a time consuming and involved process due to the differences in naming conventions and lack of associated semantics. Furthermore, due to the lack of a precise retrieval capability, the volume of information retrieved from a single query can be excessive, requiring the users to spend valuable time sorting through large amounts of irrelevant or duplicative data. Transmission of such excessive data also unnecessarily consumes throughput capacity. Retrieved information may also come from stovepiped sources that are not interoperable, thus making it difficult/impossible for the receiving system to use it (e.g. to merge the received information into a common operational picture). Additionally, the lack of a dynamic capability to monitor and control bandwidth utilization greatly inhibits a commander's ability to make timely resource reallocation decisions. Finally, while new systems are providing a tremendous increase in information availability, the commonality or interfaces to permit the cross-flow of this information among the systems are inadequate. The results are wasted capacity, increased redundancy, decreased interoperability, incompatible standards and formats, and reduced cross-functional and/or organizational information flow.

3. Fielding new IT, especially in a networked environment, is a complicated and challenging endeavor for both the mission application users and IT support staff. Security vulnerabilities in one system impact all connected systems and could allow access and sabotage of other interacting systems. The lack of proper

integration with existing systems and/or viable logistics support to include life-cycle maintenance and ongoing training can quickly erode the capabilities of the IT systems.

B. Computing

1. Process
   a. Current information systems cannot support warfighter requirements for distributed processing due to interoperability and security limitations. This situation particularly impacts dispersed operations, such as wide-area air and missile defense, where a coordinated operational picture and weapons employment is essential.
   b. Collaborative processing capabilities are very limited, which in turn, limits the ability of commanders and their dispersed components to plan efficient operations.
   c. The current set of applications does not deliver the levels of functional and technical interoperability required by DoD. This situation hinders DoD's ability to conduct effective planning, collaboration, and operational execution across the battlespace.
2. Store
   a. Users and producers cannot rapidly index/catalog, store, search, and retrieve required information. This shortfall constrains the commander's decision-making ability because essential accurate information is not available in a timely manner to facilitate decision superiority.
   b. Currently, DoD does not have a prescribed storage standard that would provide the optimum capability across DoD to store, search, and retrieve data in an expedient timeframe with appropriate quality or the ability to identify associated information or data element classification level. Therefore, commanders at all levels are unable to acquire essential information from data repositories on which to base operational and tactical decisions. This capability is essential to achieve decision superiority.

C. Communications

1. Transport
   a. DoD faces significant challenges as it attempts to meet rapidly expanding information transport requirements. This situation further exacerbates the current bandwidth shortage resulting in a restricted ability to support the command decision process.
   b. Bandwidth capacity is significantly limited across the strategic, operational, and tactical levels. Solutions exist for bandwidth problems at the strategic and, possibly, the operational levels through new technology (broadband initiatives), but at the tactical levels, this bandwidth shortage is expected to

remain into the foreseeable future. Current disparities between bandwidth needs and available capacity lead to warfighters not training as they will fight.

c. The ability to move digital information seamlessly is reduced by the current use of proprietary protocols. In addition there is a lack of prescribed DoD transport standards and a failure to conform to those DoD standards that do exist. This constricts the flow of essential information to commanders and weapons systems thus impeding time-sensitive operations across the battlespace.

d. Current DISN communications infrastructure (e.g. Non-secure Internet Protocol Router Network – NIPRNET and Secure Internet Protocol Router Network - SIPRNET) does not meet many of the GIG requirements for quality of service (QoS), bandwidth availability, and transmission priority management; thus the DISN must be enhanced to meet these stated requirements. This shortcoming greatly impedes the exchange of both unclassified and classified information across the GIG to meet warfighter requirements.

e. There is a duplication of transport media and mismatches in bandwidth and other transport requirements caused by multiple transport systems based on classification levels.

D. Presentation – Human GIG Interaction Function

1. Human-GIG Interaction (HGI)

a. The ability to present information to the human user is reduced by the heavy reliance on the use of text message formats and the inability to provide multimedia presentations. Computer systems and devices are currently tailored to interface primarily with only two human senses: sight and sound. The requirement manually to read voluminous textual material manually slows the decision-making process.

b. The inability to process multiple languages of both spoken language and applications limits the effective presentation of information. This situation is particularly constraining in allied and coalition operations, which constitute a vast majority of the operations involving the U.S. military today.

c. Systems lack the capability to ascertain the context in which humans are functioning, and thus provide information in a predetermined way rather than in the form most useful to the human given the role, mission, and function assigned. Lacking the ability to present information in the most effective and efficient manner for human use impedes military processes requiring human–system interaction.

d. Current systems are non-adaptive to user needs and cognitive styles. The systems are often non-intuitive in meeting the users' requirements and are not user friendly. Lack of this ability to present information in the most effective and efficient manner for human use slows all military processes

requiring human–system interaction and has a direct effect on a commander's effective decision-making ability.

e. There are no effective automated means for users to locally prioritize information inputs and flexibly control the ways and manner in which information is presented to them for review/alert. This limits operators' ability to modify their information receipt and notification to correspond to the operational situation. There is also a possibility that in some cases, the receipt of time-critical survival information could go unnoticed because of this shortfall.

E. Network Operations (NETOPS)

1. Network Management (NM)

a. There is a lack of asset visibility resulting in an inability to effectively manage the overall network to support common user needs. The limited network visibility is significantly impacted by the large number of stovepiped and legacy systems. Stovepiped and legacy systems are normally not designed to support global, end-to-end network management or adhere to a prescribed set of standards for interoperable use across DoD and the Intelligence Community. However, there are dedicated/specialized systems that are required to accomplish specific command missions, but do not support or facilitate effective network management of these systems.

b. There are no common prescribed standards for common user systems/networks that would facilitate network management across DoD/IC. This shortfall precludes effective network management, which is essential to ensure the most efficient and effective exchange of information across the battlespace.

c. There is no distributed network management capability that would allow the management of common user networks from more than just one central location.

d. Existing network management is currently unable to provide a fully integrated multilevel security network.

e. DoD has little or no network management capability to accompany its increasingly widespread use and application of advanced mobile wireless computing and networking which are inherently ad hoc.

f. There is no prescribed standard joint network management capability for JTF component-level common user systems/networks. Deployed network management suffers from a loosely federated approach for employing government unique (formerly government-off-the-shelf (GOTS)) and COTS software.

g. Current end-to-end communications, especially in the last tactical mile, are not fully integrated and interoperable. Specific issues include heterogeneous

network design, inconsistent firewall implementations and varying network management policies and tools.

2. Information Dissemination Management (IDM)

   a. Most military information systems are designed to support the collection, analysis, storage, and distribution of non-time-critical planning information instead of time-critical survival information. This can seriously impede the flow of survival information to those for whom it can mean life or death.

   b. There is insufficient capability to produce and disseminate time-critical survival information to specific warfighters based on a set of static information profiles, much less a set of situational dependent profiles. This can seriously impede the flow of survival information to those for whom it is critical based on their dynamically changing operational situation.

   c. Users lack visibility to available information/data. This shortfall seriously restricts the ability of commanders and decision makers at all levels to acquire information essential to making operational and tactical decisions. Having the right information at the right time and at the right place is essential for achieving decision superiority.

   d. Producers cannot make information easily available to the user in a desired format. This causes users to spend precious time reformatting and converting received information, which has the overall effect of restricting the command decision-making process and can adversely affect the success of military operations. When decisions must be made in seconds, it is essential that information arrive in a format that a user can immediately utilize.

   e. Users have a limited means to easily access information without prior knowledge of exact locations where the information is stored. This shortfall constrains the commander's decision-making ability, because essential accurate information is not available in a timely manner.

   f. Commanders have a limited ability to visualize the flow of information into and within their area of responsibility (AOR). Therefore, commanders have limited ability to inject guidance to dynamically adjust their communications infrastructure priorities with respect to a changing operational environment.

   g. Users cannot easily create or dynamically adjust their user profiles to allow for better flow of information. Therefore, commanders are unable to adjust their information requirements to ensure the receipt of critical information. This is essential in today's warfighting environment where conditions are constantly changing.

   h. Few automated means for prioritization of information exist to ensure that high priority information requests are handled first. This is particularly crucial to the delivery of survival information to designated users in critical tactical situations.

i. Current systems do not allow for the dynamic routing of information to the most efficient communications pathway available. Creating efficient communication pathways will ensure network optimization.

j. There is limited awareness of user information requirements due to inconsistent, non-interoperable, and antiquated methods of communicating these requirements to information producers. This can greatly restrict commanders' ability to acquire essential information in a timely manner.

k. There is limited status provided to information users to allow visibility into the progress of satisfying their information requirements. Therefore, commanders and their subordinates lack the ability to forecast when key information might become available, if at all, to support critical military decisions. Awareness is also limited by a lack of adequate direct communications between the information producer and the user in order to conduct problem solving, add information context and resolve ambiguities in information context.

3. Information Assurance (IA)

a. Currently there is very limited flexibility and adaptability of information security to support multilevel security operations, which can greatly impede effective command and control of military operations by restricting the availability of needed information to key decision makers.

b. Available IA technology solutions are not capable of providing effective protection against the full range of potential cyber threats. This places at risk our entire command decision-support capability on which practically all military operations rely.

c. Information systems are vulnerable to passive intercept attacks, which include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing identification (ID) numbers and passwords. These efforts can give adversaries indications and warnings of impending actions.

d. Information systems and information content are inherently vulnerable to insider attacks by malicious authorized users, which can seriously compromise the command decision process at all levels by removing or constricting automated decision support capabilities.

e. There is the lack of a capability to monitor or restrict access to sensitive/classified information by cleared persons having the appropriate need to know and to prevent the unauthorized transfer of sensitive/classified information across networks running at different classification levels. Therefore, commanders at all levels are limited in their ability to acquire essential information from data repositories and to base operational and tactical decisions on that information.

CHAPTER IV REQUIRED CAPABILITIES

A. Introduction

1.General

The primary purpose of this chapter is to describe GIG capability requirements. Capabilities are listed within seven fundamental functions (process, store, transport, human-GIG interaction, network management, information dissemination management, and information assurance), organized into four general categories (computing, communications, presentation and network operations). Because the GIG operates as a globally interconnected, end-to-end, interoperable system of systems, all systems that comprise the GIG should be GIG-enabled to allow "plug and play" interoperability among systems. A system will be considered GIG-enabled if it has the capabilities described in this chapter for the seven GIG functions, as appropriate and necessary to fulfill the system's operational purpose(s)/mission(s). The term "GIG-enabled" is used in a manner similar to that of the commonly used terms "Internet-enabled" and "Web-enabled."

2.Technology Change Management

a. Synchronization. Information technology is evolving at a rapid rate. Program Managers implementing GIG-enabled systems should plan to take advantage of technology changes. This is, sometimes, easier said than done. The rate of change in information technology is two-to-three times faster than the multi-year acquisition cycle. This means that many information technology programs deliver products/systems that are often a generation behind what is available in the commercial sector – before they get fielded they are "legacy" systems.

b. Standards and Proprietary Technology. A large percentage of information technology solutions are commercial products – many times available in the market place before the industry has settled on a "standard." A perfect example is Beta vs. VHS videocassette technology. A more current example would be the evolving standards development for eXtensible Mark-up Language (XML). Also, some companies seek to maintain a competitive economic advantage through proprietary technologies. While these solutions may satisfy an operational requirement, they most always create interoperability problems. Program Managers need to consider commercial standards when implementing GIG solutions with a view toward understanding that standards are necessary but not sufficient to ensure interoperability among systems.

c. Configuration Management. Introducing new technology into operational environments requires rigorous configuration control. Commanders and decision makers at all levels of command must have complete confidence in the information technology they use to maintain situational awareness or

commit forces. Often, backward compatibility to legacy systems will be required and should be considered as part of the new system design. Conversely, the infusion of new technology may involve process re-engineering. GIG-enabled systems should be flexible enough to accommodate such change.

d. In the final analysis, successful implementation of the GIG depends in large part on how well technology change is managed to allow us to take advantage of current and future innovations in information technology.

B. GIG Capability Requirements

1. Introduction

This section describes the GIG capability requirements, which are shown in *italics* under each GIG functional area. These requirements are intended to address the major shortfalls presented in Chapter III. All percentages stated within this MA ICD as performance measurement criteria for measuring capability requirement satisfaction are calculated against Threshold levels. A comprehensive checklist is provided in Appendix F for CDD/CPD writers to use in completing their CJCSI 3170.01B-mandated capability requirements crosswalk to ensure compliance with the GIG MA ICD as appropriate/applicable. It is important to note that these requirements are not meant to constrain the GIG. On the contrary, they are intended to promote interoperability among GIG systems. The introductory section of the GIG MA ICD Compliance Checklist addresses how CDD/CPD authors should go about determining whether a system is a part of the GIG, and thus subject to GIG MA ICD compliance, or not. The section also discusses what compliance entails in terms of a system being GIG-enabled with those information capabilities necessary to ensure that system-to-system, end-to-end external information exchanges can be carried out successfully and in an interoperable manner.

2. Computing: Process Function

a. General. Although computer-based processing is inherently involved in the execution of all GIG functions, the requirements outlined in subparagraphs (b) through (v) below are biased toward computing processes used for manipulating data, information, and/or knowledge into the desired form to support decision making and other GIG-supported activities. The capabilities detailed in the following paragraphs are aimed at alleviating interoperability, collaborative process, and security shortfalls identified in Chapter III.

b. Processing Efficiency and Effectiveness. The stated capability assumes that resources available for computing and dissemination are finite and constrained. This assumption holds true for all computing environments. Therefore, *all computing processes of systems shall optimize the use of constrained computing and dissemination resources* (***Threshold***). Based on the specified requirements, process efficiency can be traded off with process

effectiveness. If the marginal benefit of utilizing additional resources exceeds the cost of resources used, then effectiveness of processing should prevail on the process efficiency.

c. Reuse of Information Products. *Systems' previously generated, shareable information products (i.e. processed data) shall be reused to maximize consistency and efficiency, and to minimize process redundancy* (***Threshold***). Use of computing resources to reprocess raw data to regenerate information that is currently available and accessible within the GIG environment should be avoided. Besides being efficient, elimination of redundant processing promotes consistency in the processing of raw data.

d. Processing Mode. *Systems shall have processes that accommodate an interactive and multimedia processing environment within the GIG* (***Threshold***). *Systems' need for processing modes other than interactive and multimedia, especially batch processing, shall be clearly demonstrated and justified prior to their adoption* (***Threshold***). *Systems shall use time-critical processing when dealing with survival information in order to meet stringent timeliness requirements* (***Threshold***).

e. Cohesiveness. *Each process of a system shall accomplish a well-defined, single function, so as to achieve a high degree of cohesion and enhance process reusability and system maintainability* (***Threshold***). Cohesiveness is an internal characteristic of process design and generally leads to modular and maintainable systems. It also promotes process reusability. Cohesion can range from low to high, where the low is characterized by coincidental cohesion and high is characterized by functional cohesion. On the low side, the tasks performed by a process are either very loosely related or may also be unrelated to one another. A high degree of cohesion implies that the process is performing one distinct procedural task.

f. Modularity. Non-modular processes are monolithic and complex. Hence, computing processes designed to be modular are typically small in size, simple to understand, exhibit high cohesiveness and use simple interfaces to interact with other processes. Simplified interfaces imply low coupling and lead to relatively independent processes. *Systems' processes shall be modular to reduce maintenance and promote reusability* (***Threshold***). Modularity allows processes to be treated as "black boxes," which enables plug and play systems and operational architectures.

g. Process Reusability. *Systems shall have, to the maximum extent possible, processes that are designed (using off–the–shelf standard components built according to an open standard) and implemented to be reusable in multiple systems and computing environments as plug and play "commodities" or "generics" rather than custom built from scratch each time* (***Threshold***).

h. Reliability. *Systems shall have processes that are classified either as deterministic or non-deterministic, with each deterministic process producing consistent and definite results, and each non-deterministic process specifying*

a range with boundary limits and the expected average for each output generated (***Threshold***).

i. Validation. *The accuracy of outputs from systems' processes, deterministic or otherwise, shall be testable, meaning that processes shall be executable and the actual outputs generated by a process shall conform to expected outputs governed by operational requirements* (***Threshold***). *In the case of systems' non-deterministic processes, it shall also be possible to predict all outputs within specified limits* (***Threshold***). The output limits used for validation will match the output limits specified for process reliability.

j. Verifiability. *Systems shall have processes that facilitate verification and verification activities shall be performed to discover design errors and demonstrate the conformity of the system to the specified requirements* (***Threshold***). Conformance to the specified requirements establishes a traceable path from the designed and implemented system to the specified functionality of the system. This allows the system developer to demonstrate that the system is doing what it was specified to do. It is imperative that all processes facilitate verification activities. Verification and validation differ in their objectives. Verification is a check for building the system the right way regardless of whether it is the right system or not, whereas validation ensures that the right system was built. Verification is also instrumental in eliminating costly errors during early stages of the development process, which eventually results in reduced maintenance costs.

k. Interprocess Communications (IPC). *To achieve interoperability among systems' processes, all processes shall use standardized mechanisms to communicate with each other, and process interfaces shall follow established standards for interprocess communications regardless of whether they are communicating with processes residing within the same computing system or with processes residing on remote systems* (***Threshold***). IPC standards should be followed for all process-to-process communications with the exception of embedded IT, which include data exchange, service request, and remote invocation. Also, standards used by a process for interprocess communication should not be dependent on the characteristics of the remote process. Similarly, it should be a material consideration for IPC, whether the remote process is a part of a legacy system, resides within the GIG environment, or resides outside the GIG boundary.

l. Process Prioritization. *Systems' processes shall be responsive to task prioritization dynamically* (***Threshold***). Computing processes that are common across multiple tasks should be responsive to the priority attached to the task regardless of the mechanism used for establishing the task priority. It will be assumed that the task priorities can be changed dynamically and therefore the process should also be capable of changing its response to task prioritization dynamically.

m. Process Adaptability. Processes should not make any absolute assumptions about available computing and communication resources. *All critical*

processes of systems shall have the capability to monitor the available resources and dynamically adjust their processing characteristics and behavior in accordance with the resources made available for their use (***Threshold***).

n. Standards-Based Processing. *All processes of systems shall demonstrate compliance with existing directives, instructions, and prescribed standards, to include appropriate performance-based standards* (***Threshold***). When appropriate, decisions regarding the applicability of directives or instructions will be biased toward those most widely used directives and instructions in the GIG environment. DoD prescribed industry, international, Federal Information Processing Standards (FIPS), NATO STANAGS, and MIL-STANDARDS will be used by the GIG.

o. Process Security. *All processes of systems shall be protected and secured at appropriate levels and be visible to and cooperate with all information assurance operations* (***Threshold***). This implies that access to a process should be controlled, with only authenticated users allowed to access a process. The level of security associated with the process should be appropriately justified. It will depend on the sensitivity of the task being accomplished by the process and governed by a formally established security policy.

p. Non-GIG Interoperability. If and when required, processes residing in the GIG environment should be capable of interfacing with processes residing on non-GIG systems while retaining GIG security and integrity and should not degrade the non-GIG system's security and integrity. *Systems' processing shall accommodate non-DoD* (***Threshold***) *and allied and coalition* (***Objective***) *operations when necessary.*

q. Robust and Flexible Processing. *All process failures and processing exceptions of systems shall be handled through error-handling and recovery mechanisms that are consistent with threat and risk levels associated with the processing task* (***Threshold***).

r. Analytical and Collaboration Services. *Systems' processing shall support analytical and collaboration capabilities through services that support collaborative planning, decision making aids, modeling and simulation, data mining, intelligent agents, and virtual workspaces* (***Threshold***)***.***

s. IM Support. *Systems' processing shall accommodate all Information Management (IM) tasks related to creation, acquisition, transmission, organization, storage, dissemination, presentation, protection, and disposition of information* (**Threshold**).

t. Interface Definition. *All process interfaces of systems shall be well defined and clearly specified, to include at a minimum, all input specifications, output specifications, and specifications for controls required for triggering the process* (***Threshold***).

u. Cross-Platform Functionality. *Systems' processes shall be independent of the computing platform regardless of the programming or scripting* (***Threshold***).

v. Process Availability. *Systems' processing components shall ensure that the overall system availability is not compromised due to run-time process failures* (***Threshold***).

3. Computing: Store Function

a. General. The store function is responsible for the retention, organization, and disposition of information to facilitate information sharing across the GIG. The capabilities detailed in the following paragraphs will offset shortfalls described in Chapter III by enabling and supporting the indexing, cataloging, and storage of information and the rapid search and retrieval from repositories, all of which are essential for decision superiority.

b. Data Interoperability. *Systems shall identify and use common standards for data and metadata representation* (***Threshold***). When a standard exists, the developer will use the standard. In cases where standards do not exist for a class of data that is being stored, the developer will be responsible for unambiguously defining both the syntax and semantics. *All of a system's data that will be exchanged, or has the potential to be exchanged, shall be tagged in accordance with the JTA/DISR standard for tagged data items (e.g., Extensible Markup Language [XML], the current JTA/DISR standard), and tags shall be registered in accordance with the DoD Metadata Registry and Clearinghouse policy and implementation plan (**Threshold, KPP**).*

c. Information Integrity.[6] *Systems' storage process shall not alter stored data in a manner that compromises the integrity of the data/information* (***Threshold***). Compression and other similar storage techniques should be authorized as long as the information the user retrieves from the storage process has not been altered or changed from the information that was placed in storage.

d. Infrastructure Management. *Systems shall provide visibility of storage infrastructure to efficiently manage the available storage capacity and provide the capability to remove/discard/update stored data as required* (***Threshold***).

e. Data Distribution. *Systems' data shall be stored in a manner that facilitates its distribution in accordance with processing and transport needs and supports the rapid retrieval of the information by the user* (***Threshold***). *Each item of systems' stored data shall have a single, discrete source of reference, so that future updates of that data, while being stored in other locations, will be able to refer back to the designated single reference source, thus ensuring that the information is being updated with the most current available version* (***Threshold***).

f. Data Survivability. *Systems' data shall be stored in a manner that assures the required access to and use of all needed data, and in a way that prevents*

[6] Used synonymously with the term "data integrity."

the loss of stored data from physical threats such as fire, water damage, information operation threats, power outage, natural events, and Electromagnetic Pulse (EMP) as appropriate to the information being stored (***Threshold***).

g. Data Security. *Systems' data being stored shall include its classification and releasability criteria within the semantic tag or associated schema* (***Threshold***).

h. Data Disposal. *Systems' data that is no longer required shall be disposed of effectively and efficiently, so that the storage space that was used by the disposed data can be used for the storage of new data without the user having to do any additional actions once the decision to dispose has been made* (***Threshold***).

i. Data Retention. *Systems' data shall be retained in a manner that meets all mission and regulatory guidance and is transparent to the user* (***Threshold***). Short-term retention should meet operational needs of the warfighter and long-term retention should meet legal or other regulatory requirements.

4. Communications: Transport Function

a. General. Transport is the movement of information and/or knowledge among users, producers, and intermediate entities. The capabilities detailed in the following paragraphs will work to alleviate transport shortfalls identified in Chapter III by improving Quality of Service (QoS) through the implementation of DoD transport standards, and reducing duplication of transport functions. While these improvements may not totally offset the shortage of available bandwidth in the face of expanding information transport requirements, these enhancements should go far to improve the current situation.

b. Switching/Routing/Transmission. *To ensure the unimpeded exchange of information that is necessary to meet user requirements, systems providing switching, routing, and transmission control capabilities/mechanisms shall be fully interoperable and work seamlessly across the entire GIG, in accordance with the DoD JTA/DISR* (***Threshold***).

c. Spectrum Supportability/Electromagnetic Environmental Effects**.** *Systems shall optimize the use of the electromagnetic spectrum through efficient frequency reuse and advanced modulation, compression, and filtering techniques, and shall comply with DoD, National and International spectrum management policies as applicable* (***Threshold***). *Systems shall be mutually compatible with other systems, including allied and coalition systems, in the operational environment and shall not be degraded by electromagnetic environmental effects* (***Objective***).

d. Quality of Service (QoS). Emphasis on superior QoS commensurate with each user's requirements must be an overarching GIG operating principle. *Transport systems shall provide QoS capabilities that ensure information identified as priority is delivered ahead of regular traffic 99 percent of the time*

(***Threshold, KPP***) *and ahead of regular traffic 99.9 percent of the time* (***Objective, KPP***). Required QoS factors include:

- Prioritization. *End users shall be able to assign priority to information targeted for transport* (***Threshold***).
- Response Time. *All transport capabilities shall be designed to meet or exceed customer stated expectations for response times* (***Threshold***).
- Precedence. *Data shall receive expedited handling during transport in accordance with the commander's policy and user assigned priority* (***Threshold***).
- Reliability. *Delivery of information shall be guaranteed in accordance with its assigned service level* (***Threshold***).
- Latency. *It shall be possible to deliver information in real and/or near real time* (***Threshold***).

e. Information Integrity. *Systems shall maintain and guarantee during transport the integrity of all information elements exchanged throughout the GIG to enable user confidence; information integrity shall be 99.99 %* (***Threshold, KPP***) *and 99.999 %* (***Objective, KPP***).

f. Standards. *To ensure system interoperability across the GIG and to support assured uninterrupted service, all transport capabilities shall be standards-based using DoD JTA/DISR,* unless waived in accordance with the waiver process described in DoD 5000.2-R (latest version) (***Threshold***)**.** It is only through the rigid enforcement of and compliance with such standards that fully GIG-wide information exchange will be possible.

g. Connectivity. *Transport systems shall provide connectivity on demand to all fixed and deployed locations/users* (***Threshold***)**.** This on-demand, seamless connectivity is essential to satisfy the rapidly changing requirements of warfighters at all levels engaged in operations throughout the world. Unimpeded mobility, while maintaining uninterrupted connectivity both laterally and vertically, is a basic requirement of the 21st century warfighter. This is essential given the combination of a shrinking force structure and the ever-increasing missions and locations where our military forces are required to operate. *Transport systems shall have the ability to maintain network connectivity on-the-move to meet both Service and JTF requirements in all warfighting environments (afloat, sub-surface, airborne, in space, and on the ground)* (***Objective***).

h. Capacity. *With minimal exceptions, GIG transport capacity shall be viewed as an open system that is available to transport information from all domains utilizing either unicast, multicast, and/or broadcast techniques wherever necessary to provide information on demand to the warfighter/decision maker* (***Threshold***)**.** *Transport systems shall have the reserve capacity to accommodate surge loading and support multiple military operations as described in Defense Planning Guidance* (***Objective***).

i. Technology Insertion. To effectively keep pace with advances in technology that have the potential to render existing systems obsolete shortly following acquisition*, the GIG shall enable and support the seamless and efficient insertion and incorporation of emerging (future) technologies into the transport domain* (***Threshold***). Such a technology insertion provision is essential to maintain the operational effectiveness of the GIG.

j. Security. *Systems shall provide link and transmission security based on the level of risk acceptable to the user, and the GIG security architecture shall support use of clear headers if and when necessary* (***Threshold***).

k. Robustness. Transport system reliability is a fundamental requirement for ensuring necessary information exchanges to support military operations. Single points of failure are a primary concern in any transport architecture. *To avoid any single point of failure, the GIG shall use multiple connectivity paths (not susceptible to the same threats) and media* (***Threshold***).

l. Scalability. Modern military force deployment scenarios require varying force levels depending on the particular mission and associated operational requirements. Therefore, *transport capability shall be scalable and adaptable to meet the dynamic needs of users* (***Threshold***).

m. Survivability. *Transport systems shall be protected against all potential threats commensurate with the operating environment and the criticality of the information being transported, and shall also ensure connectivity through the total threat environment (i.e., conventional and nuclear*) (***Threshold***).

n. Availability/Reliability. *To be effective, transport capabilities shall be available to provide reliable information exchange services to the warfighter/decision maker on demand and shall be responsive to the criticality of the information to be exchanged* (***Threshold***).

o. Tactical Deployability. Military tactical forces require maximum mobility and ease of deployment. This requires that their supporting systems also be easily transportable. Therefore, *transport systems supporting tactical forces shall minimize lift requirements and be transportable using existing JTF/Service notional lift capabilities* (***Threshold***).

p. Transport Element Status. *All transport elements (e.g. switches, routers, etc.) shall be capable of providing status changes to network management devices by means of an automated capability in near real time 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) of the time.*

q. Secure Voice Interoperability. *Strategic and tactical secure voice systems shall be interoperable, with a 99%* (***Threshold, KPP***) *and 99.9%* (***Objective, KPP***) *call throughput success rate.* Throughput success/failure is defined as a call completion rate when both secure voice systems are operational and available.

r. Secure Voice with Allied and Coalition Forces. *Secure voice cryptography shall be provided to or developed with allied forces to enable interoperability* (***Threshold***)**.** *Secure voice systems shall be interoperable with coalition*

forces (***Objective***). *A secure voice system shall be able to be provided to coalition forces that is interoperable with the U.S. version using coalition releasable technology* (***Threshold***).

s. Information Over Tactical Data Links. *Systems transporting/exchanging information over tactical data links (TDLs) shall use one or more members of the J-Series Family of Tactical Data Links in accordance with the DoD Joint Tactical Data Link Management Plan (JTDLMP) and the DoD Joint Technical Architecture (JTA/DISR) (**Threshold**).*

5. Presentation: Human-GIG Interaction (HGI) Function

a. General. HGI is the input and output of information representations between human(s)-in-control and GIG entry point(s). The system design should minimize human performance errors, interface problems, and workload (physical, cognitive, attention) requirements. Interface characteristics should be chosen to maximize human productivity and performance as verified by iterative testing. Parametric thresholds and objectives for acceptable human performance should be established in CDDs/CPDs. The capabilities detailed in the following paragraphs will alleviate shortfalls described in Chapter III by making systems more user friendly and better adapted to users' cognitive styles. The use of multimedia presentations will reduce the need for reading voluminous textual material that can slow the decision-making process. Users will be able to prioritize information inputs and control the manner in which information is presented to them for review/alert. All of these improvements will greatly enhance a commander's decision-making ability.

b. Output/Input. *Systems' HGI shall present information to and accept information from humans using a combination of visual, aural, tactile, and/or other unique sensory methods* (***Threshold***). Presentation requirements need to encompass new methods of output as well as more advanced graphical displays, animation, and immersive technologies such as virtual realities. Software download capabilities that provide basic user-assisted functionality such as metadata encoding, converters, fonts, rendering, and input method editors should be available as needed.

- Visual Presentation. Visual methods should be selected from the full spectrum of means, simple to complex, as suggested by blinking lights and plain text through full-motion, stereoscopic, color imagery and human visual inputs. Seventy percent of the body's sense receptors cluster in the eyes.
- Aural Presentation. Audio methods should be selected from the full spectrum of means, simple to complex, as suggested by a single constant tone through multi-language, stereophonic, synthesized speech.
- Tactile Presentation. Tactile methods should be selected from the full spectrum of means, simple to complex, as suggested by simple applications of pressure and/or vibration to complex patterns of pressure, temperature, and vibration.

c. Feedback. *Systems' HGI shall provide unobtrusive confirmations of user input and actions, to include implicit visual, aural, and/or tactile feedback in response to user actions (e.g., push-button highlighting, mouse button or keyboard key clicks, or audible tone) as well as explicit notifications that entered data was properly entered, accepted by the system, and/or errors were detected* (***Threshold***).

d. Specialized Environments. *Systems' HGI shall functionally accommodate use in an NBC or other specialized operating environment, as designated by mission needs* (***Threshold***). Systems used in tactical environments should be designed to prevent any form of compromise to the safety of users. Not all user interfaces will be required to operate in all possible operating environments. Other specialized environments may include cockpits, mobile environments (e.g., tanks), hand-held radios, ships, low light, etc.

e. Usability. *Systems' HGI shall be usable by all end-user skill levels in the aspects of learnability, flexibility, and tailorability, which shall be verified by iterative user testing* (***Threshold***). Parametric thresholds and objectives should be established by the CDD/CPD. Measures of effectiveness and measurable performance criteria should be defined by determining system usability during user evaluation and tests.

- Learnability. Systems' HGI should minimize the time and effort required to reach a specified level of user performance. The specified level of performance should be system-specific based on mission needs.
- Flexibility. Systems' HGI should maximize the extent to which the system can accommodate changes to the end-user tasks beyond those initially specified. This includes providing multiple methods of accomplishing a task for various skill levels or user preferences.
- Tailorability. Systems' HGI should maximize the extent to which the system can accommodate mission changes, user preferences, or experience level as well as the specific needs of the presentation device.

f. Task Efficiency. *Systems' HGI shall provide decision aids and tools, as necessary, to maximize user efficiency and performance of their task, with operator aids designed to support specific user tasks and tailored to the information needs of the targeted user* (***Threshold***).

g. User-Centered Design. *A user-centered design process and user testing shall be employed for systems' HGI to ensure that the end-user's cognitive frameworks and expectations are accommodated by the system design* (***Threshold***). A user-centered design process, executed early during system development through a series of user evaluations and refinements, ensures that the requirements of the end-user are satisfied and results in increased user satisfaction with the final system.

h. Standards. *Systems' HGI shall be compliant with the DoD JTA/DISR* (***Threshold***).

i. Neutrality. *Systems' HGI presentation format shall not change the intended meaning of the information being presented; thus all data shall be clearly labeled to avoid misinterpretation or confusion* (***Threshold***).

j. Ergonomics. *To minimize user fatigue and discomfort, systems' HGI hardware and software elements shall be ergonomically designed with respect to the user's operating environment* (***Objective***).

k. Errors. *Systems' HGI shall be designed to minimize user input, mechanical, and perception errors and support recovery from errors* (***Threshold***).

l. On-line Help. *Systems' HGI shall provide context-sensitive on-line help tools for use at the user's request, thus eliminating/reducing the need for off-line support or documentation that may distract the user from the intended task* (***Threshold***)**.**

6. Network Operations (NETOPS)

Network Operations is the organizational and procedural structure used to monitor, manage, and control the Global Information Grid by means of the GIG functions of Network Management (NM), Information Dissemination Management (IDM), and Information Assurance (IA). To effectively support network-centric warfare (including collaborative planning) key parts of these functions must be integrated. Commanders (e.g., at the theater and enterprise level) must have situational awareness of network IT assets and the information flow across echelons. Separate management of some NM, IDM, and IA functions is also necessary.

a. Network Management (NM) Function

(1) General. Network Management is the set of activities that establishes and maintains the GIG network switching, transmission, information services, and computing resources available to fulfill users' telecommunications and connectivity needs and demands. NM services are fault, configuration, account, performance, and planning management. The capabilities detailed in the following paragraphs will alleviate shortfalls described in Chapter III by enabling and supporting distributed and partitioned network control, the implementation of standards, and enhanced asset visibility. These enhancements will result in greatly improved overall NM.

(2) GIG End-to-End Situational Awareness. Network managers, on behalf of commanders, must have real time knowledge of the network. This knowledge must encompass awareness of all aspects of the network, including all network assets, their physical location, and their logical relationship within the network. *To accomplish GIG end-to-end situational awareness, systems shall have the NM capability of automatically generating and providing an integrated/correlated presentation of networks and all associated network assets* (***Threshold***).

(3) Dynamic, Predictive Planning. *Systems shall have the NM capability to perform dynamic, predictive planning by gathering, storing and using*

knowledge about GIG assets/resources, so as to optimize their utilization (***Threshold***). Knowing equipment types and quantities available to support an operation is imperative for GIG utilization planners. Initially, a database must be defined and populated with organizations and their known GIG assets/resources. Once defined and populated, the database should have the capability to be modified, as required, to support changing mission requirements to include activation/deactivation. The network management system should include network design and engineering functions that account for all voice, video, and data networks that could comprise a proposed system, including commercial technology. These functions should include automated mapping of network topology; measurement and recording of traffic flow data; trend analysis; spectrum planning and management; propagation analysis; electromagnetic resolution; and electronic key management. A modeling and simulation capability should be provided to allow a planner to assess the impact of changes to a system or network, without interrupting the operational network. *Systems shall have the NM capability to create/modify/distribute GIG network plans and orders in accordance with user requirements* (***Threshold***).

(4) Distributed and Partitioned Network Control. *Systems shall have the NM capability to transfer control rapidly of one or more objects or groups of varying size, and reestablish control when relinquished without hindering end-to-end visibility by the senior network manager, while maintaining continuous control* (***Threshold***). Only one designated active manager for a network object should be permitted at any given time. However, oversight of managers of network objects may shift as forces/assets are apportioned, allocated, or assigned without requiring a change of the active manager.

(5) Remote Object and Network Control and Configuration. Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status. Networks comprising the GIG are evolutionary in nature and generally are comprised of both legacy and emerging systems, some with their own management systems. *Systems shall have a NM capability that leverages existing and evolving technologies and has the ability to perform remote network device configuration/reconfiguration of objects that have existing DoD JTA/DISR management capabilities* (***Threshold***).

(6) Network Status. Components of the GIG provide metrics to network managers to allow them to make decisions on managing the network. *Systems shall have an automated NM capability to obtain the status of networks and associated assets in near real time 99%* (***Threshold, KPP***) *and 99.9%* (***Objective, KPP***) *of the time.*

(7) Automated Fault Management. *Systems shall have the NM capability to perform automated fault management of the network, to include problem*

detection, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving (***Threshold***). This capability allows network managers automatically to monitor and maintain the situational awareness of the network's manageable devices, and to become aware of network problems as they occur based on the trouble tickets generated automatically by the affected object or network. Alarms will be correlated to eliminate those that are duplicate or false, initiate test, and perform diagnostics to isolate faults to a replaceable component.

b. Information Dissemination Management (IDM) Function

(1) General. Information Dissemination Management should be utilized to maximize the flow of relevant information to the user, consistent with the user's information requirements, the commander's policy (to include statutory requirements), and available resources. The capabilities detailed in the following paragraphs will alleviate shortfalls described in Chapter III by enhancing the capability to produce and disseminate time-critical survival information to specific warfighters. It will provide awareness of, access to, and delivery of information in desired formats across the GIG based on the priority of information flows set by the commander's dissemination policy, infrastructure availability, and security policies. The value of IDM increases as the access to information increases and the hierarchical relationships of information flow control are well established between the commanders within and between AORs. Additionally, the value of IDM increases as the user's specific information requirements are articulated, because the information producers can be more proactive and efficient in satisfying these requirements. IDM dependencies include robustness of the networks/communications transmission pathways, the systems on which IDM will reside, and the standardization of data, databases, and data description (metadata). Specific IDM requirements are described in sub-paragraphs (2)-(30) below.

(2) Requirement Identification. *Systems shall have an IDM capability to assist users in efficiently defining their information requirements in a manner that captures key attributes associated with these requirements (e.g., timeliness, quantity, confidence level, etc.)* (***Threshold***). This capability will facilitate rapid awareness of existing information that could satisfy the information requirement. It will also trigger the need to collect new information, minimize information overload, and optimize use of available communications resources. This capability will provide a means of tracking and retrieving available information consistent with information and mission requirements in a manner that most effectively utilizes resources at the national, regional, and local levels.

(3) Search Driven Information. *Systems shall have an IDM capability to acquire needed information by search queries, with successful searches yielding 85% of available, needed information based on the user query, and with no more than 20% of the received information being*

irrelevant/unusable (waste) or failed searches (***Threshold, KPP****); and yielding 95% of available, needed information and with no more than 10% of the received information being irrelevant/unusable (waste) or failed searches* (***Objective, KPP***). The key to achieving a successful search is a well-defined user query. *Systems shall have an IDM capability to locate and characterize available information of interest that minimizes information overload* (***Threshold***).

(4) Information Advertisement. *Systems shall have an IDM capability through which an information producer's products become known to the user population* (***Threshold***).

(5) Quality of Advertisements. *Systems shall have an IDM capability that will enable information producers to describe their information products accurately using established search words and level of description 90% of the time (**Threshold**).*

(6) Product Descriptions. *Systems shall have an IDM capability that enables information producers to label their products using standardized metadata (including classification) (**Threshold**).*

(7) Source Cataloging. *Systems shall have an IDM capability that enables information producers to automatically build catalogs of information products and product updates based on available information products and users' profile requests (**Objective**).*

(8) Profile Management. *Systems shall have an IDM capability that supports building profiles based on collaboration of information requests from users (through their profile requests), the commander's IM policy, and on information producers applying appropriate rule sets (e.g. security) (**Threshold**). Systems shall have an IDM capability that enables profiles to be transferable and reusable (**Threshold**). Systems shall have an IDM capability that enables automatic recognition of a change in Commander's Dissemination Policy (CDP) during profile creation, alerting the customer to that change and adjusting/modifying the profile to conform to the CDP (**Threshold**).*

(9) Profile Driven Information. *Systems shall have an IDM capability that enables the user to identify information requirements (**Threshold**). Systems shall have an IDM capability that, once a profile is posted, enables information producers to automatically disseminate a minimum of 95% of available, needed information, with no more than 15% of the information received being irrelevant/unusable (waste) (**Threshold**); and a minimum of 99% of available, needed information, with no more than 10% of the information received being irrelevant/unusable (waste) (**Objective**).*

(10) Filtering of Multiple Sources. *Systems shall have an IDM capability that provides a means to filter out superfluous information to the level of fidelity as determined by the local commander (**Threshold**).*

(11) Geographic Areas. *Systems shall have an IDM capability that enables information producers to disseminate information to a specific geographic area and to the users who are within that area (**Threshold**).*

(12) Commander's Dissemination Policy Generation. *Systems shall have an IDM capability that provides a means for assisting commanders in rapidly building effective and intuitive information dissemination policies, and automates readjustment of subordinate commands' dissemination policies with appropriate alerts to those commands that policy has changed (**Threshold**).*

(13) Information Flow Awareness. *Systems shall have an IDM capability through which commanders become aware of the information flowing within their AOR to facilitate adjustments to meet operational mission requirements* (***Threshold***). *Systems shall have an IDM capability for monitoring and tracking information flows to identify trends; for forecasting volume, content, and QoS consistent with information and mission requirements; and for predicting the results of information control policies to optimize available resources consistent with mission priorities* (***Objective***).

(14) Allied Access. *Systems shall have an IDM capability that supports US/allied (**Threshold**)/coalition (**Objective**) accessibility to information, conforming to a commander's dissemination policy and DoD and IC security regulations.*

(15) Status. *Systems shall have an IDM capability to track and report the status of the satisfaction of information requirements from the point of information request to delivery of requested information* (***Threshold***).

(16) Resource Monitor. *Systems shall have the capability to monitor and control IDM core services and distribute system status information to IDM administrators (**Threshold**).*

(17) Controlled Access. *Systems shall have an IDM capability to regulate access to information in accordance with information assurance policies and procedures, and a commander's dissemination policy, to include the ability to constrain/control the awareness of the existence of information* (***Threshold***). Specific dissemination policy will constrain browsing by those under a commander's command based on variables such as file size, type, source, classification level, resource, classification level or location.

(18) Information Description. *Systems shall have an IDM capability to access information from the GIG using standard metadata* (***Threshold***).

(19) Delivery Plan. *Systems shall have an IDM capability to build an end-to-end delivery plan based on user information requirements, mission priorities, dissemination policy, and available transport resources* (***Threshold***). *Systems shall have an IDM capability to dynamically adjust delivery plans based on changes to user information requirements,*

mission priorities, dissemination policy, and available transport resources (***Objective***).

(20) Information Retrieval. *Systems shall have an IDM capability to retrieve information of interest once it has been located* (***Threshold***).

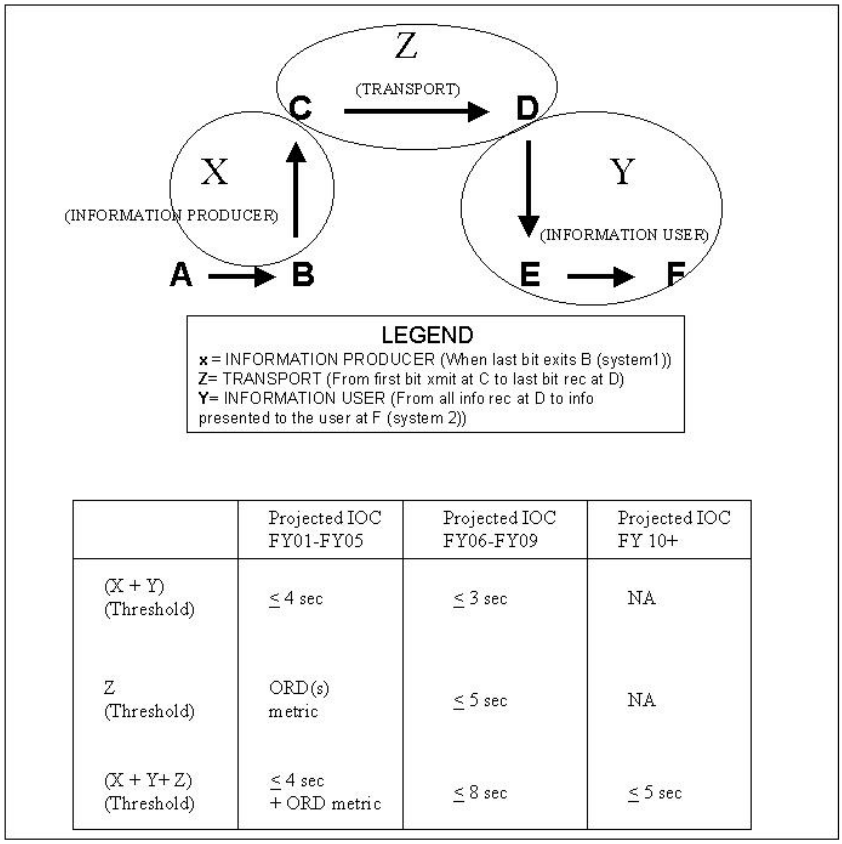
(21) Collection Request. *Systems shall have an IDM capability to request the collection and production of information that is required by a user but is not already available via search-driven query* (***Threshold***).

(22) Dynamic Profiling. *Systems shall have an IDM capability to activate/deactivate information requirements based on external influences such as mission, role, time, location, situation, and environment* (***Threshold***).

(23) Delivery Management. *Systems shall have an IDM capability to assign attributes (e.g., priority, QoS) to information that will govern its dissemination and also a capability to convey the attributes (e.g., priority, QoS, etc.) of information to the transport system* (***Threshold***). Individual information elements may have varying degrees of importance/criticality for identifiable users/groups of users. In recognition of this fact, *systems shall have an IDM capability to assign precedence to information, which will govern its dissemination throughout the GIG, and ensure that the priority for an information requirement shall be carried with all the elements of information required to satisfy that requirement, to include the capability to apply precedence to blocks of information packets for digital voice service to ensure adequate QoS* (***Threshold***).

(24) Policy Management. *Systems shall have an IDM capability for commanders, and those delegated information flow authority within an organization, to dynamically adjust their information dissemination policies* (***Threshold***)**.** None, some, or all components of a commander's dissemination policy may be specified. In other words, a commander may choose not to restrict access and may only assign priorities to information flows when information/communication resources are exceptionally scarce. Using IDM, a commander must be able to quickly modify a policy in response to changes in operational situations or communications resources. This enables the effective control of information to keep pace with the user's needs in the dynamic environment in which he or she is operating.

(25) Survival Information Dissemination. *Systems shall have an IDM capability that, utilizing a standard schema, IAW the commanders' dissemination policies and user profiles, will support the means for prioritization of information flows within a theater, using theater apportioned resources, and enable dissemination of survival information (limiting survival information to less than 12 kb) within the timeframes of the matrix portrayed in Figure 5, 95% of the time* (***Threshold, KPP***) *and 0.5 seconds 95% of the time* (***Objective, KPP***).



	Projected IOC FY01-FY05	Projected IOC FY06-FY09	Projected IOC FY 10+
(X + Y) (Threshold)	≤ 4 sec	≤ 3 sec	NA
Z (Threshold)	ORD(s) metric	≤ 5 sec	NA
(X + Y+ Z) (Threshold)	≤ 4 sec + ORD metric	≤ 8 sec	≤ 5 sec

Figure 5. Survival Information Dissemination Metric

(26) Correlation. *Systems shall have an IDM capability to minimize the delivery of redundant information, as well as the capability to identify complementary, parallel, or reciprocal relationships among information elements* (***Threshold***).

(27) Notification. *Systems shall have IDM capabilities* (***Threshold***) *for notification of:*

- *changes in policy*
- *changes in user information requirements*
- *information becoming available or changing*
- *changes in network status that impact information flow*
- *changes in provider and user system status*
- *the delivery/receipt of information*
- *status of IDM services*
- *product availability*
- *a conflict within the delivery plan*

Systems shall have an IDM capability that gives the user the option of being notified when information related to his/her requirements becomes

available or when changes occur; in the case of survival information, notification will be automatic (***Threshold***).

(28) Flexibility. *Systems shall have IDM capabilities that can be applied from the strategic to the tactical levels without major software modifications* (***Threshold***).

(29) Scalability. *Systems shall have IDM capabilities that are scalable to meet system and operational user requirements* (***Threshold***). For example, a man-portable tactical communications and computing system would include some but not all of the IDM capabilities available on a major command center C2 system.

(30) Directory Services. *Systems shall have an IDM capability that provides directory services with minimal personal intervention* (***Threshold***).

c. Information Assurance (IA) Function

(1) General. Information Assurance is defined as information operations that protect and defend information and/or information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and response capabilities. The capabilities detailed in the following paragraphs will alleviate shortfalls described in Chapter III by enhancing protection against the full range of potential cyber threats.

(2) Information Integrity and Availability. The GIG must be an assured system of systems with a defined and controlled security perimeter. Interconnection of GIG systems/elements to outside systems/elements should be done only in a controlled fashion using adequate assurance means. The GIG must include a protected electronic perimeter for local enclaves in accordance with *Defense in Depth standards* (*CJCSI 6510.01C*). Therefore, *systems shall have the IA capability to define, control, and defend enclave boundaries* (***Threshold***). *To support IA across the GIG, systems shall be robust, survivable and capable of rapid restoration* (***Threshold***). *Systems shall have an IA capability that provides users with timely, reliable access to processes and data even in the event of a denial of service attack* (***Threshold***). *Systems shall also have the IA capability to ensure information and process integrity throughout the system (during storage, processing, transmission and presentation) so as to prevent unauthorized or unintended changes, in accordance with mission specific criteria* (***Threshold***).

(3) Prevent Opportunity to Attack. *Systems shall be developed in accordance with Defense in Depth standards (CJCSI 6510.01C) to prevent or at least minimize the opportunity to attack; and shall have, in the event of attack, the IA capability to immediately define, detect, and respond appropriately to anomalies/attacks/disruptions from external threats, internal threats and natural causes* (***Threshold***).

(4) Access Control. *Systems shall have an IA capability that provides adequate protection from user attempts to circumvent system access controls, accountability, or procedures for the purpose of performing unauthorized system operations* (***Threshold***).

(5) Detection and Responses. *Systems shall incorporate a detection, reporting, and response IA infrastructure that enables rapid detection of and reaction to all sources of anomalous events and enables operational situation awareness and responses* (***Threshold***).

(6) Security Domains. *Systems shall have an IA capability for operating within each security domain and across any security domains, while ensuring that all operations comply with existing DoD and IC security requirements* (***Threshold***).

(7) Authentication/Confidentiality/Non-repudiation. *Systems shall meet and maintain minimum IA Defense in Depth standards, including certification and accreditation in accordance with the DITSCAP process (e.g., CJCSI 6510.01C, DoDI 5200.40)* (***Threshold, KPP***). *Systems shall utilize/interoperate with security management and the DoD public key infrastructure* (***Threshold***). *Systems shall provide proof of information origin and receipt as required* (***Threshold***).

(8) Confidentiality Services. It is essential that secure operations can be conducted across security domains. *To support this, systems shall have an IA capability that ensures information is not disclosed to unauthorized entities or processes on the network and infrastructure so as to protect against passive intercept attacks, including unauthorized disclosure of information and traffic analysis* (***Threshold***). *Systems shall also have an IA capability to share data among users operating at different and/or multiple security levels as appropriate (e.g., one terminal with multiple security modes, "colorless" backbone, data labeling, allied/coalition, unclassified through TS/SCI) and at the same time protect the data from unauthorized disclosure* (***Threshold***).

(9) Content-Based Encryption. *Systems shall have an IA capability to perform content-based encryption of information objects at the host instead of depending on the bulk encryption of the entire network in order to secure the information* (***Threshold***), *and this capability shall also be available for operations involving allied and coalition forces* (***Objective***).

C. Interoperability

Interoperability is the ability of two or more systems, units, or forces to provide services to and accept services from other systems, units or forces to enable them to operate effectively together. This condition is achieved between communication-electronics systems or equipment when information or services can be exchanged directly and satisfactorily between users. The degree of interoperability that can be achieved will be determined primarily by the accomplishment of the IER fields in

Appendix G. To comply with the interoperability KPP mandated by CJCSI 6212.01B, *systems shall satisfy all critical IER attributes to the threshold level* (***Threshold, KPP***) *and satisfy all IER attributes to the objective level* (***Objective, KPP***). NOTE: Because this document represents a conversion of the GIG CRD to a GIG Mission Area ICD, it is still considered a "legacy" Joint Requirements Document that, per CJCSI 6212.01C dated 20 November 2003, must continue to use the Interoperability KPP (I-KPP). However, also per direction of CJCSI 6212.01C, CDDs and CPDs initiated six months after the Instruction's publication date (on or after 21 May 2004) must include a Net-Ready Key Performance Parameter (NR-KPP) with associated metrics and performance measures, in lieu of the I-KPP. In light of this, Appendix H, "Net-Ready Key Performance Parameter (NR-KPP) Compliance Guidelines" is provided herein to assist CDD and CPD authors in preparing a NR-KPP that properly addresses interoperability within a GIG capabilities context. Appendix H offers specific guidance and assistance in understanding net-centric attributes and capabilities required to move into the net-centric environment in the GIG, and in determining and documenting NR-KPP compliance. The Appendix contains relevant material excerpted from Enclosures F through G of CJCSI 6212.01C; from Chapter 7 of the Defense Acquisition Guidebook, "Acquiring Information Technology and National Security Systems;" and from the OSD NII/DCIO Net-Centric Checklist. The latest version of the Defense Acquisition Guidebook can be found at **http://dod5000.dau.mil/** and the most current version of the Net-Centric Checklist is located at the NII Document Archives site at **http://www.dod.mil/nii/doc/** (a listing of Net-Centric Attributes can also be found at this site).

D. Key Performance Parameters.

The capability requirements shown in the Table 4-1 KPP Rollup below are essential for achieving interoperability, both inside the GIG and external to it.

Table 4-1. KPP Rollup

FUNCTIONAL AREA	CAPABILITY	REQUIREMENT
Interoperability	Satisfy Critical IER Attributes	Systems shall satisfy all critical IER attributes to the threshold level (**Threshold, KPP**) and satisfy all IER attributes to the objective level (**Objective, KPP**).
Store	Data Interoperability	All of a system's data that will be exchanged, or has the potential to be exchanged, shall be tagged in accordance with the JTA/DISR standard for tagged data items (e.g., Extensible Markup Language [XML], the current JTA/DISR standard), and tags shall be registered in accordance with the DoD XML Registry and Clearinghouse policy and implementation plan

FUNCTIONAL AREA	CAPABILITY	REQUIREMENT
		(**Threshold, KPP**).
Transport	Quality of Service	Transport systems shall provide QoS capabilities that ensure that information identified as priority is delivered ahead of regular traffic 99% of the time (**Threshold, KPP**) and 99.9% of the time (**Objective, KPP**).
	Information Integrity	Systems shall maintain and guarantee during transport the integrity of all information elements exchanged throughout the GIG to enable user confidence; information integrity shall be 99.99 % (**Threshold, KPP**) and 99.999 % (**Objective, KPP**).
	Transport Element Status	All transport elements (e.g., switches, routers, etc.) shall be capable of providing status changes to network management devices by means of an automated capability in near real time 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) of the time.
	Secure Voice Interoperability	Strategic and tactical secure voice systems shall be interoperable, with a 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) call throughput success rate.
Network Management	Network Status	Systems shall have an automated NM capability to obtain status of networks and associated assets in near real time 99% (**Threshold, KPP**) and 99.9% (**Objective, KPP**) of the time.
IDM	Search Driven Information	Systems shall have an IDM capability to acquire needed information by search queries, with successful searches yielding 85% of available, needed information based on the user query and with no more than 20% being irrelevant/unusable (waste) or failed searches (**Threshold, KPP**); and yielding 95% of available, needed information and no more than 10% being irrelevant/unusable (waste) or failed searches (**Objective, KPP**).

FUNCTIONAL AREA	CAPABILITY	REQUIREMENT
	Survival Information Dissemination	Systems shall have an IDM capability that, utilizing a standard schema, IAW the commanders' dissemination policies and user profiles, will support the means for prioritization of information flows within a theater, using theater apportioned resources, and enable dissemination of survival information (limiting survival information to less than 12 kb) within the time frames of the matrix portrayed in Figure 5, 95% of the time (**Threshold, KPP**) and 0.5 seconds 95% of the time (**Objective, KPP**).
Information Assurance	Authentication/ Confidentiality/ Non-repudiation	Systems shall meet and maintain minimum IA Defense in Depth standards, including certification and accreditation IAW the DITSCAP process (e.g., *CJCSI 6510.01C*, *DoDI 5200.40*) (**Threshold, KPP**).

CHAPTER V OPERATIONAL ENVIRONMENT-THREAT

A. General

1. A detailed discussion of the foreign threat to the GIG does not exist. However, GIG-related threats are addressed in several DIA-validated, published documents: *Automated Information Systems Threat Environment Description (TED)* (U), NAIC-1574-0210-00, Sep 00, (S/NF); *Military Satellite Communications (MILSATCOM) Systems Threat Assessment Report (STAR)*, NAIC-1574-0367-00, Feb 01, (S/NF); *Electronic Warfare Threat Environment Description (TED)* (U), NAIC-1574-0731-01, Feb 01, (S/NF); and *Worldwide: Threats to Network Centric Warfare* (U), ONI-1573-001-00, October 1999 (S/NF). Additional relevant DIA documents: *Information Operations Threat to the Defense Information Systems Network (DISN) DI-2710-6-01, March 2001* (U), *Information Operations Threat to the Military Use of Commercial Satellite Communications* DI 2710-25-01, February 2001 (U), *Information Operations Threat to the Secret Internet Protocol Router Network (SIPRNET)* NIE 2000-16-I, February 2001 (U), and a *National Intelligence Estimate on the Cyber Threat to the U.S*, NIE 2000-16-I, December 2000. The President's Commission on Critical Infrastructure Protection published its findings in October 1997. This unclassified document discusses the threat to the U.S. critical infrastructure, including telecommunications; electrical power systems; gas and oil production, storage and transportation; banking and finance; transportation; water supply systems; and emergency services. This chapter focuses the threat discussion on the IT concerns of the GIG.

2. Threats to Critical Infrastructure. Many adversaries believe the best way to avoid, deter, or offset U.S. military superiority is to develop capabilities that threaten the U.S. homeland. In addition, our national infrastructure is vulnerable to disruptions by physical and computer attack. The interdependent nature of the infrastructure creates even more of a vulnerability. Foreign states have the capability to attack the GIG infrastructure. They possess the intelligence assets to assess and analyze infrastructure vulnerabilities, and a wide range of weapons, to include conventional munitions, weapons of mass destruction (WMD), and information operations tools to take advantage of those perceived vulnerabilities.

3. The most immediate and serious infrastructure threats are from trusted insiders, terrorists, criminals, and other groups or individuals who are positioned to conduct well-coordinated strikes against selected critical nodes. While conventional munitions attacks are most likely now, over time our adversaries will develop an increased capacity, and willingness to employ WMD. They are also likely to enhance their capabilities for information warfare operations. COTS products and seamless services present new security challenges and concerns, providing opportunities to develop software functions that allow unauthorized access, theft and manipulation of data, and denial of service.

4. Skilled adversaries may be able to conduct pre-attack exploitation and attack preparations with nearly undetectable signatures, thereby minimizing indications and warning of their intentions. Any potential adversary is apt to target specific

information about the GIG in order to exploit or disrupt its operations. An adversary may target specific interconnections around the world, its end-to-end set of information capabilities, or the GIG's associated processes and personnel.

5. Threats to allies may become a threat to the GIG, even though the GIG may not be the primary target. Connectivity and interoperability with coalition, allied and non-DoD users and systems suggests an expanding universe of potential insider threats to consider. Because the GIG uses commercially available systems, widely available attack tools are becoming increasingly capable and deployable by people with fewer technical skills than previously required. One may expect adversaries to develop asymmetric responses to perceived vulnerabilities.

6. One form of asymmetric warfare to be considered is information operations (IO). Potential state-level adversaries could use IO tactics to enable military advantage, political and/or financial gain, and/or damage. Increased challenge, status, and/or thrills may motivate foreign non-state actors, such as hackers, to intrude into GIG systems. Evidence suggests that a successful attack against the GIG must be narrowly focused and precisely coordinated. Disrupting the entire GIG for an extended period of time is an unlikely event. In addition to IO, WMD threats are an expanding asymmetric threat to GIG operations. More information on these threats is contained in *Proliferation of Nuclear, Biological, and Chemical Weapons and Ballistic Missiles: A Primer*, DI-1569-20-99, December 1999 (S/NF).

B. Information Operations Threat

1. The primary tactical threat to the GIG comes from information operations (IO) . Supported by intelligence exploitation, the IO threat includes the following tactics: computer network attack (CNA), computer network exploitation (CNE), electronic warfare (EW), perception management, and physical attack.

2. Adversaries recognize our civilian and military reliance on advanced information technologies and systems, and understand that information superiority provides the United States with unique advantages. Accordingly, potential foes could pursue IO capabilities as a relatively low-cost means to undermine public and political support for U.S. actions, attack key U.S. capabilities, and counter U.S. military superiority.

3. The IO threat continues to spread worldwide, with more mature technologies and more sophisticated tools being developed continuously. However, the level of threat varies widely from adversary to adversary. Most opponents currently lack the foresight or the capability to fully integrate all IO tools into a comprehensive attack. Many, with limited resources, will seek to develop only CNA options relying on modest training, computer hardware and software purchases, and/or the use of "hired" criminal hackers. At present, many nations have programs to protect their own information systems, and some, particularly Russia and China, are believed to have offensive information operations capabilities.

4. DoD systems are regularly probed and scanned as prerequisites to exploitation and/or attack, via foreign locations in order to define network architectures and assess vulnerabilities. Intelligence exploitation of the GIG can occur easily from

various sources. Technical collection and analysis may provide adequate pre-attack information, such as data flow analysis and GIG architectural details. Technical collection tools are widely available and increasingly user friendly.

5. CNA and CNE tactics can be used against the GIG's computer systems, operating systems, and software applications. CNA and CNE include stealing passwords and data, inserting malicious code, denial of service (DOS), and data corruption, modification, and manipulation. The well-publicized distributed DOS attacks against several U.S.-based commercial Web sites have sensitized foreign countries to their own vulnerabilities against this type of attack.

6. EW tactics can be used against the GIG's wireless segments. Few commercial products provide electronic protect (EP) technology that could provide some defense against electronic attack (EA) and electronic support (ES) tactics. The rapid global growth of commercially available wireless communications systems has caused some countries to be interested in developing EW tactics against those systems, not necessarily against the United States. However, when common systems are used, then foreign EW may impact U.S. systems.

7. Perception management and physical attack may be used against GIG personnel and facilities, including not only those controlled by United States personnel in host nations, but also those portions controlled by foreign personnel in host nations. Radio frequency (RF) weapons, such as electromagnetic pulse (EMP) and directed energy weapons (DEW) can be used to physically disrupt electronic circuits. Foreign interest in protecting their own systems against these weapons can lead to increased understanding of the capabilities of RF weapons.

C. Future Threat Trends

1. As DoD increasingly uses COTS technology and systems, the threat to unprotected systems will continue to grow. However, a primary impetus behind the globalization of information technology is electronic commerce, which will require improved information security (INFOSEC). Therefore, DoD may benefit from the global need for improved INFOSEC to enable personal privacy in electronic commerce and banking.

2. CNA/CNE tools will continue to grow in capability while the required level of user experience and knowledge to use them effectively decreases. These tools will become increasingly available on the Internet. Additionally, one would expect to see more automated tools, such as the distributed DOS tools that use hundreds or thousands of previously exploited computers in a coordinated attack. Implementing the Defense-in-Depth strategy will minimize the reaction time to these emerging threats. Continued efforts will be needed to support Computer Network Defense (CND) efforts to reduce vulnerability to the increasing potential threats. Defensive IO ensures the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives.

3. EW systems, especially ES systems, will continue to be produced, marketed, and exported around the world. As U.S. and global use of digital wireless networks

grows, expect continued interest in intercepting and exploiting these systems. Some systems that are being marketed for law enforcement applications also have potential military use. Foreign critical infrastructure protection against EW threats will continue to expand.

Appendix A MA ICD Supporting Analysis

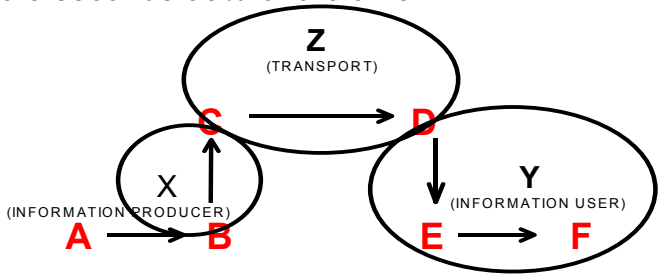
Analysis Supporting the Delivery of Survival Information.

This analysis supports the establishment of a 5 seconds or less threshold requirement for survival information delivery. This analysis was originally done for the IDM CRD (now retired), and then incorporated into the GIG CRD and included herein as part of the GIG MA ICD.

Unclassified

Survival Information Dissemination KPP

Utilizing a standard prioritization schema, IAW the commanders' dissemination policies and user profiles, IDM will support the means for prioritization of information flows within a theater, using theater apportioned resources, and enable dissemination of survival information (limiting survival information to less than 12 kb) within the time frames of the matrix portrayed below 95% of the time (Threshold) with an objective of 0.5 seconds 95% of the time.



	Projected IOC FY01-FY05	Projected IOC FY06-FY09	Projected IOC FY10+
(X+Y) **(Threshold)**	≤ 4 sec	≤ 3 sec	NA
Z **(Threshold)**	ORD(s) metric	≤ 5 sec	NA
(X+Y+Z) **(Threshold)**	≤ 4 sec +ORD metric	≤ 8 sec	≤ 5 sec

LEGEND
X = INFORMATION PRODUCER (When last bit exits B (system 1))
Z = TRANSPORT (From first bit xmit at C to last bit rec at D)
Y = INFORMATION USER (From all info rec at D to info presented to the user at F (system 2))

1

UNCLASSIFIED

Introduction

It was determined that in order to support the ORD writers in developing their requirements to pass "survival" types of information that a baseline metric was required. The primary purpose of the analysis was to determine what the appropriate baseline metric for the delivery of "survival" type information should be. The analysis was focused primarily on three areas:

Current Commercial Delivery Speeds (What is Possible)

The first area (section I) examined the information delivery speeds supported by commercial communications systems and their impact on future DoD information technology (IT) systems. The analysis also looked at the extent of DoD's current use of leased commercial systems/technology and the potential impact on information delivery times by the use of those systems/technology now and in the future.

Existing Delivery Speeds for DoD Systems (What We Do Today)

The second area (section II) examined existing DoD systems (example provided is JTIDS) and determined what information delivery speeds they currently support. As a result of our analysis we found that JTIDS using 1970's technology can deliver "survival" information in less than 2.5 seconds. In addition, the analysis looked at the cost of information delivery times in terms of the warfighter's battlespace.

IER Analysis (Service ORDs Today)

The third area (section III) examined the inconsistencies between the timeliness metrics in current transport and user system (non-transport) ORDs (section I). The analysis looked at the timeliness requirements of non-transport ORDs and matched those up against the transport ORDs relied on or information dissemination. The ORDs were reviewed to determine if the baseline delivery timeliness metrics in the transport ORDs were sufficient to support the survival information delivery timeliness requirements specified in the user system ORDs and vice versa.

Section I. Current Commercial Capabilities and Implications for IDM and GIG CRDs

The intent of the analysis outlined in this section is to describe the current capabilities of the commercial communications sector in moving information around the globe. It is not intended to compare current military systems against these standards, but to demonstrate what is possible now using currently existing technology. It is reasonable to assume that we would want future military systems to move toward the current technical capabilities as we develop new systems in the future and take advantage of these improvements. Today DoD currently leases 100% of the DISN backbone infrastructure from the commercial sector and in doing so takes advantages of the delivery speeds that commercial communications vendors can provide. It is also key to understanding the potential information delivery speeds of the future and to remember that as we continue to adopt commercial off the shelf (COTS) solutions we gain the advantages of commercial technology in our military solutions.

The current information delivery capabilities provided by the commercial sector are highlighted in Figure 1-1 below. The speed of roundtrip transmission between London and

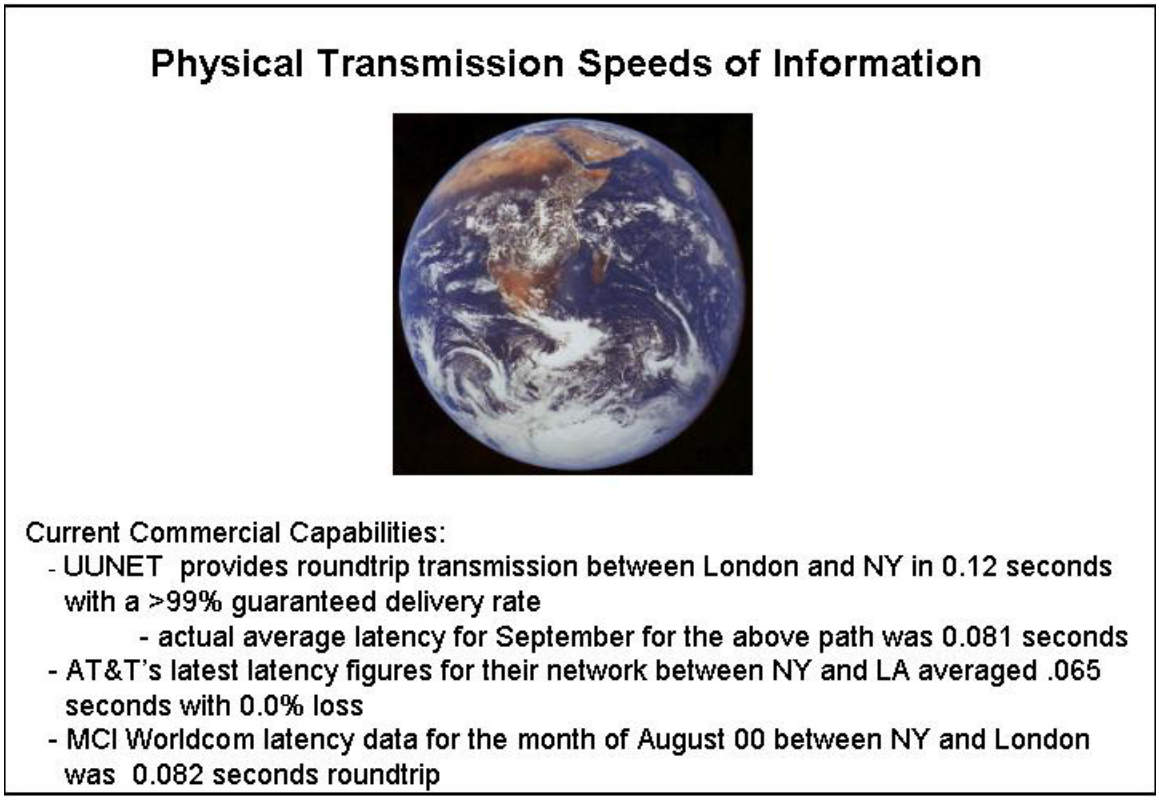


Figure 1-1 Physical Transmission Speeds of Information.

NY as currently advertised, by the commercial carrier UUNET, is 0.12 seconds with a 99% guaranteed delivery rate. The actual average delivery time over this path for

the month of September was in fact as low as 0.081 seconds. It should be noted that all the commercial carriers are consistent with their delivery speeds. For example, the average latency over the same route for the month of August 2000 by a different carrier, MCI-Worldcom, was 0.082 seconds roundtrip.

The delivery times show the current information capabilities and should serve as a guideline for the development of future DoD systems, which would be using the same commercial technology.

Today DISA's DISN, with its leased commercial backbone, is capable of achieving speeds of delivery as demonstrated in Figure 1-1. As an example during the NATO air campaign in Kosovo, DoD leased commercial circuits from CONUS to forward bases in Italy. Figure 1-2 illustrated the potential delivery times using the current commercial delivery times available from UUNET between CONUS and Italy. In this example, to deliver the information from Italy to the actual user in the field a geo-stationary satellite was used. This example deals only with the transport times and does not add in potential computer processing times (which in the seamless environment of the future should be negligible) between the commercial network and the satellite system.

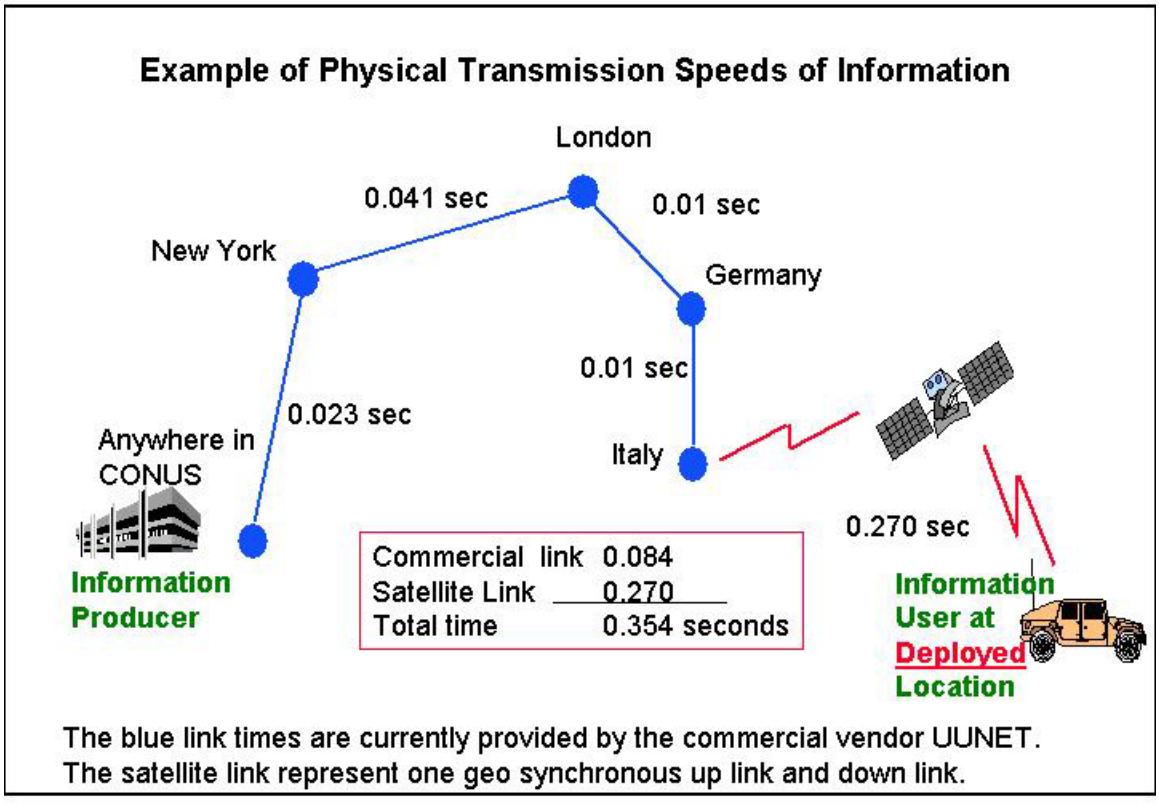


Figure 1-2 Example of Physical Transmission Speeds of Information

Furthermore, router processing times, which range in microseconds, are also not being included.

Figure 1-2 shows the speed of information delivery from an information producer located in CONUS using a commercial leased system (DISN backbone) to a forward deployed base in Italy in 0.084 seconds. The figure shows the transition of that information to a geo-stationary satellite system (0.270 seconds –satellite delay) and than the delivery of the information to a user in a deployed tactical environment. The **total transportation time is 0.354 seconds** from CONUS to the deployed user.

If a fiber optic grid existed around the globe the round trip delay for delivering information form one point on the globe to any other point and back is at most **0.2 seconds.**

Speed of light in a vacuum = 300,000 Km/sec

Speed of light in optical fiber = 200,000 Km/sec

Circumference of the earth = 40,000 Km

Total round trip delay to farthest point and back 40,000/200,000 = 0.2 sec

The purpose of this section is to demonstrate the art of possible. That is to show the current capabilities of the commercial communications sector's ability to move information with current technology. DoD, through it's leasing of commercial infrastructure for systems like the DISN backbone and the implementation of COTS technology should be able to move information in the near future in the timeframes currently being provided by the commercial sector.

Section II. Review of Existing DoD Systems

Recognizing that we often are forced to fight in areas where the communications infrastructure is far less robust, we next examined existing systems and their information delivery speeds for "survival" type information to the warfighter. The example provided below is the Joint Tactical information Distribution System (JTIDS) using 1970's technology.

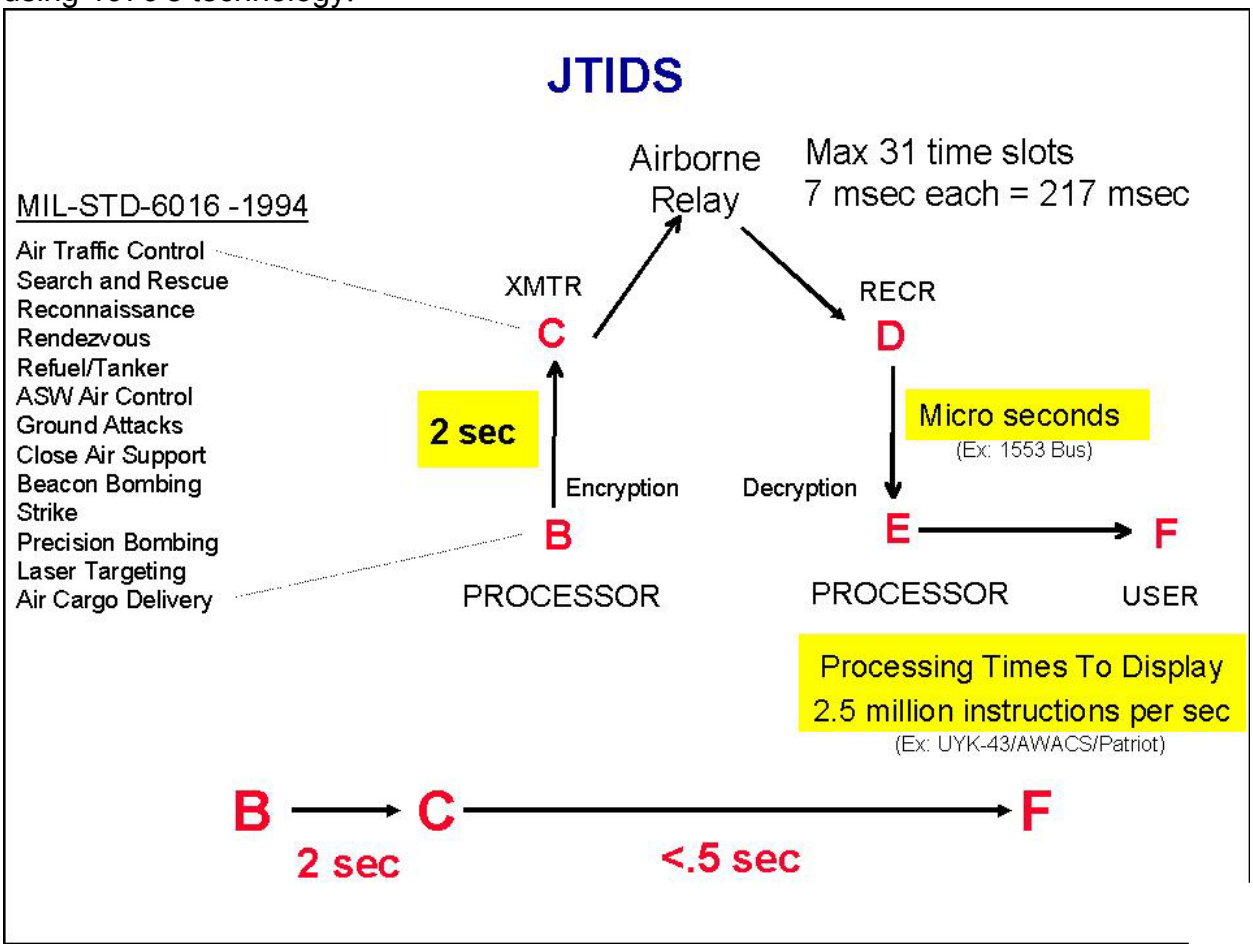


Figure 2-1 JTIDS Example of Survival Information Delivery

In the analysis of JTIDS we were able to show the flow of information out of processor B and delivered it to the user through the JTIDS system. The following is a breakdown of the time required to deliver the information:

2 seconds	IAW MIL STD 6016 time for "survival" type information is to clear the buffer in this time
0.217 sec	From Transmitter C it goes at the speed of light to Receiver D – to stress the time we added the airborne relay which added 0.217 seconds due to the max 31 time slots required time

0.000001 seconds Estimated time to cross 1553 bus in our example

0.000001 seconds processing time to display (Time estimate based on 2.5 million instructions per sec – Pentium 60)

Total time for JTIDS to deliver "survival" information from B (the point at which the information is identified as being "survival" and the user who needs it as survival can be identified) to the delivery to the user at F is **less than 2.5 seconds** using existing 1970's technology.

Warfighter Battlespace

Warfighters seek to maximize battlespace. Timeliness impacts battlespace. Using table 2.1 a 0.8 Mach missile travels over the ground at approximately 1 mile every 5 seconds. Similarly a ground threat travelling at 60 mph closes 130 meters in 5 seconds. The bottom line is faster is better in terms of impact to a warfighter attempting to engage either threat. The longer it takes to cue an unalerted operator the more battlespace is sacrificed.

Table 2-1 The Cost of Time in terms of Battlespace

THREAT SPEED	**DISTANCE TRAVELLED IN 5 SECONDS**
Incoming missile at 0.8 Mach	**1. 1 Mile**
Mobile ground threat at 60 MPH (96 KM per hour)	**2. 130 Meters**

Section III. IER Interoperability in Support of Delivery of Survival Information

The timeliness metric for survival push KPP provides a baseline attribute for follow on ORDs, which disseminate information.

Problem: Current ORD interoperability KPPs exist that cannot be achieved/measured due to inconsistencies among ORD timeliness metrics when common user transport systems are utilized and/or multiple send/receive nodes are designated.

Background: ORDs are required by CJCSI 3170.01A and 6212.01B to identify top level information exchanges that are external to the system (i.e., with other C/S/A, allied, and coalition systems). Those information exchange requirements considered critical became a part of the interoperability KPP.

Our review of ORD interoperability KPP's (examples shown below) indicate that when transport system timeliness requirements are matched up against non-transport ORDs there is often lack of agreement between the two. This could result in a major interoperability problem.

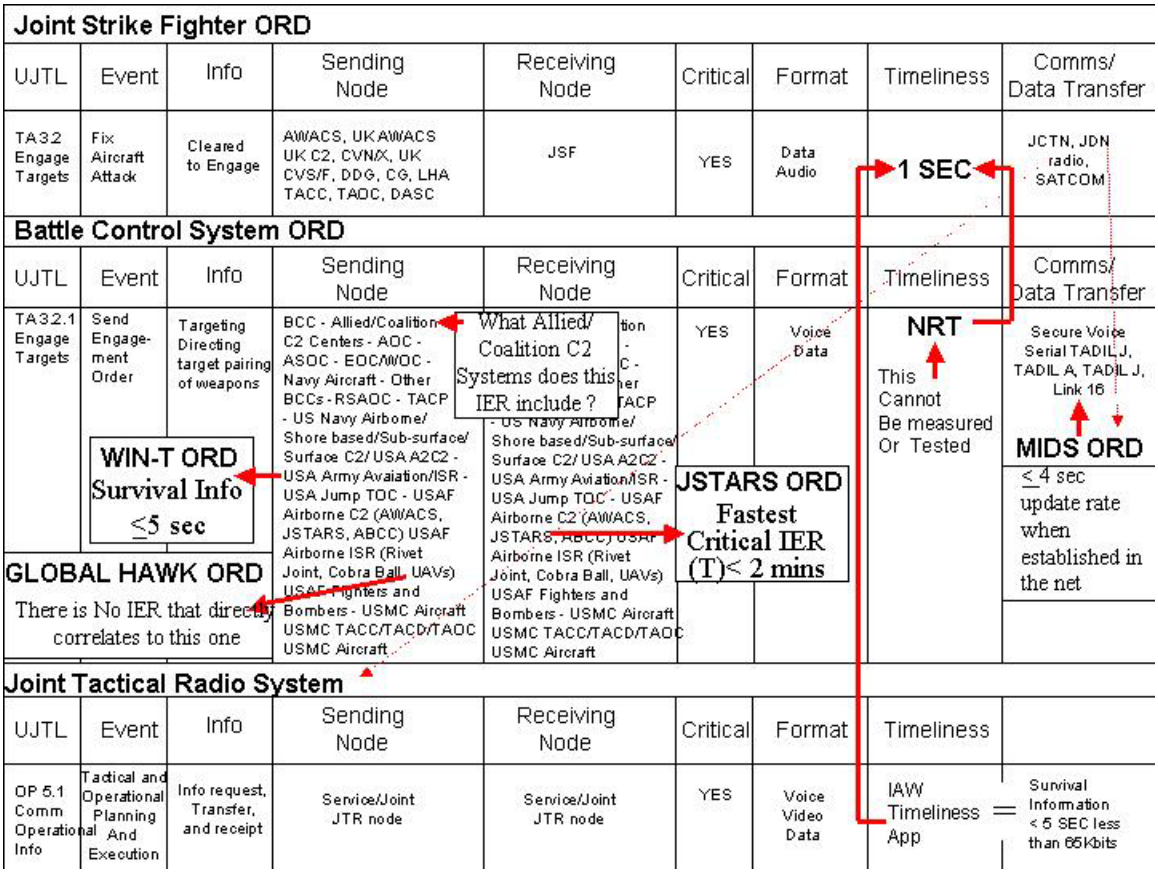


Figure 2-2 IER Timeliness Examples

In the first IER example, the JSF critical IER for “cleared to engage” cannot be met. The timeliness metric of 1 sec is unachievable because the systems used to support the delivery of the “clear to engage” information do not support the 1-sec delivery time. If JTRS and MIDS are utilized to support the radio and JDN format, then a timeliness metric of < 5 sec must be used in the timeliness field of the “cleared to engage” IER to ensure accomplishment of this critical IER.

AAAV Top Level IERs

UJTL	Event	Info	Sending Node	Receiving Node	Critical	Format	Timeliness	Class
TA3.2 Engage Targets	Perform Offensive Operations	Fire Support	AAAV(C)	SACC/TACC, ABCCC, CAS A/C Forward Air Control	YES	Voice	< 2 sec	Secret

Joint Tactical Radio System IERs

UJTL	Event	Info	Sending Node	Receiving Node	Critical	Format	Timeliness	
OP 5.1 Comm Operational Info	Tactical and Operational Planning And Execution	Info request, Transfer, and receipt	Service/Joint JTR node	Service/Joint JTR node	YES	Voice Video Data	IAW Timeliness App =	Survival Information < 5 SEC less than 65Kbits

Figure 2-3 IER Timeliness Examples

The Critical IER for fire support found in the AAAV interoperability KPP cannot meet its timeliness threshold of <2 sec if JTRS is used, because JTRS has an end to end delivery time of < 5 seconds for survival information.

Solution: In examining numerous Service System and Transport ORDs the value of ≤ 5 seconds appears to represent the lowest common denominator and may not cause adverse effect or additional cost to the Services

Examples of “Survival Type” Information found in ORDs:

Joint Strike Fighter	Engage Targets	3 seconds
Advanced Amphibious Assault	Direct Forces	< 2 seconds
UH 60 Black Hawk Mission Coordination	1-4 seconds	
WIN – T	Survival Information	< 5 seconds
V-22 Joint Multi-Mission Vertical Aircraft	Engage Targets	< 5 secs

Each of the examples provided is a **critical service/joint ORD external IER** that relies on common user communication transport systems to disseminate "survival" information.

The current transport/dissemination ORDs **also** support a timeliness metric of ≤ 5 seconds.

MIDS-LVT ORD

UJTL	Event	Info	Sending Node	Receiving Node	Critical	Format	Timeliness	Class	
TA 5.6 Employ Tactical Info Ops	Disseminate Threat Data	Situational Awareness	Any C2 participating unit Plus Non C2 Surveillance and EW	Any Participating unit	YES	Data	≤ 4 SEC Update rate	S	F-15, F-16, F/A –18 CVN, CG, DDG, LHD, LPD, B-1, B-2, B-52, Patriot, THAAD, MEADS, FAAD, ADTOC, JTAGS

Joint Tactical Radio System IERs

UJTL	Event	Info	Sending Node	Receiving Node	Critical	Format	Timeliness	
OP 5.1 Comm Operational Info	Tactical and Operational Planning And Execution	Info request, Transfer, and receipt	Service/Joint JTR node	Service/Joint JTR node	YES	Voice Video Data	IAW Timeliness App =	Survival Information < 5 SEC less than 65Kbits

SATCOM

A-EHF and MUOS state a requirement for less than 2 sec push-to-talk delay from spoken word at the transmit terminal to be received at the receive terminal

Figure 2-4 IER Timeliness Examples

Section IV. Summary

In conclusion, this analysis demonstrates that there is a need to establish a baseline to guide the ORD writers in the development of their timeliness metrics. It was shown that the commercial communications systems are capable of delivering information in timeframes that are substantially less than 5 seconds. The analysis showed that selected existing DoD systems (example provided for JTIDS using 1970's technology) can currently support the delivery of "survival" information in 5 seconds or less. It was also shown that a timeliness metric of $\leq$ 5 seconds is consistent with the ORDs that are currently being written to support the delivery of "survival" type information. Based on the analysis described in this report it should be feasible today to support the 5-second or less threshold requirement for survival information delivery.

Appendix B Integrated Architecture Products

Appendix C References

1. American National Standard for Telecommunications-Telecom Glossary 2000 http://glossary.its.bldrdoc.gov/projects/t1glossary2000
2. Annual Report to the President, Congress, Secretary of Defense, 2001: http://www.dtic.mil/execsec/adr2001
3. C4ISR Architecture Framework, Version 2.0, 18 December 1997
4. Capstone Requirements White Paper for Joint C4 to Meet the Needs of 2010 and Beyond, USJFCOM, October 1999
5. CJCSI 3170.01B, “Requirements Generation System,” 15 April 2001
6. CJCSI 3222.01, “Requirements for High Altitude Electromagnetic Pulse Protection of C3 Nodes and Systems,” 8 October 1993
7. CJCSI 6210.02, “Attack Information and Operational Architecture of the Integrated Tactical Warning and Attack Assessment System,” 15 July 1997
8. CJCSI 6211.02A, “Defense Information System Network (DISN) and Connected Systems”, May 1996
9. CJCSI 6212.01B, “Interoperability and Supportability of National Security Systems and Information Technology Systems,” 8 May 2000
10. CJCSI 6510.01C, Information Assurance and Computer Network Defense, April 2001
11. CJCSI 6811.01A, “Nuclear Command and Control System Technical Performance Criteria (NTPC),” 9 June 2000
12. Clinger Cohen Act of 1996 (Information Technology Management Reform Act)
13. Concept for Future Joint Operations: Expanding JV 2010, May 1997.
14. DARPA, AITS JPO Sources
15. DI-1569-20-99, “Proliferation of Nuclear, Biological, and Chemical Weapons and Ballistic Missiles: A Primer, “ December 1999 (S/NF)
16. DI-2710-6-01, “Information Operations Threat to the Defense Information Systems Network (DISN),” March 2001
17. DI-2710-25-01, “Information Operations Threat to the Military Use of Commercial Satellite Communications,” February 2001
18. DII Master Plan, V 8.0, “Implementing the Global Information Grid,” 24 May 1999
19. DISA’s Memorandum, “Defense Information Infrastructure Capstone Requirements Document,” 22 April 1998
20. DoD CIO Guidance and Policy Memorandum No. 8-8001, ”Global Information Grid,” 31 March 2001
21. DoD CIO Guidance and Policy Memorandum No. 6-8510, “Information Assurance,” 16 June 2000
22. DoD CIO Guidance and Policy Memorandum No. 10-8460, “Network Operations,” 24 April 2000
23. DoD CIO GIG Information Assurance Implementation Guidance, 10 April 2000
24. DoD CIO Memorandum, “GIG Definition,” 22 September 1999
25. DoD CIO Memorandum, “GIG Definition,” 2 May 2001
26. DoD Directive 4630.5, “Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C3I) Systems,” 12 November 1992

27. DoD Directive 5000.1, Change 1, “The Defense Acquisition System,” 4 January 2001
28. DoD Directive 5000.2-R (Interim), “Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs,” 10 June 2001
29. DoDD 5200.28, “Security Requirements for Automated Information Systems,” 28 March 2001
30. DoDD 8000.1D, “Defense Information Management Program,” 27 October 1992
31. DoD Instruction 4630.8, “Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C3I) Systems,” 18 November 1992
32. DoDI 5000.2, “Operation of the Defense Acquisition System,” (including Change 1), January 2001
33. DoDI 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” 7 October 1999

DoD Joint Technical Architecture: http://disronline.disa.mil/VJTA/jta_archives.jsp

34. DoN CIO IT Standards Guidance, Version 99-1, 5 April 1999: http://www.ipv6forum.org/navbar/presentations/usnavy/itsg99-1.pdf
35. Enabling the Joint Vision: http://www.dtic.mil/jcs/j6/enablingjv.pdf
36. Federal Acquisition Streamlining Act of 1994
37. Federal Standard 1037C, Telecommunications Glossary of Telecommunications Terms, National Telecommunications Information Administration, 1997
38. Global Information Grid Architecture, OASD (C3I): http://in.disa.mil/
39. Information Dissemination Management (IDM) Capstone Requirements Document (MA ICD), U.S. Joint Forces Command (USFCOM), 8 May 2001
40. “Information Assurance Technical Framework,” Release 3.0, NSA, September 2000: http://www.iatf.net/framework_docs/version-3_1/index.cfm
41. Information Assurance Through Defense in Depth, Joint Chiefs of Staff, February 2000Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” 12 April 2001
42. Joint Publication 3-13, “Joint Doctrine for Information Operations,” 9 October 1998
43. Joint Publication 6-0, “Doctrine for C4 Systems Support to Joint Operations,” 30 May 1995
44. Joint Publication 6-02, “Doctrine for Employment of Operational/Tactical C4 Systems,“ 1 October 1996
45. Joint Tactical Data Link Management Plan, June 2000
46. Joint Vision 2010: http://www.dtic.mil/jointvision/history.htm
47. Joint Vision 2020: http://www.dtic.mil/jointvision/history.htm
48. McGraw-Hill Illustrated TELECOM Dictionary, Third Edition, Jade Clayton, McGraw-Hill Publishing, 2001
49. Military Acronyms, Initials and Abbreviations: http://www.fas.org/news/reference/lexicon/acronym.htm
50. Mission Information Management (MIM) Architecture, January 2001
51. NAIC-1574-0210-00, “Automated information Systems Threat Environment Description (TED),” September 2000, (S/NF)

52. NAIC-1574-0367-00, “Military Satellite Communications (MILSATCOM) Systems Threat Assessment Report (STAR),” February 2001, (S/NF)
53. NAIC-1574-0367-00, “Electronic Warfare Threat Environment Description (TED),” February 2001 (S/NF)
54. NCSC-TG-004, Glossary of Computer Security Terms, 21 October 1988
55. NCSC-TG-016, Guidelines for Writing Trusted Facility Manuals, October 1992
56. NCSC-TG-029, “Introduction to Certification and Accreditation Concepts,” January 1994
57. NIE 2000-16-I, “National Intelligence Estimate on the Cyber Threat to the U.S.,” December 2000

NIE 2000-16-I, “Information Operations Threat to the Secret Internet Protocol Router Network (SIPRNET),” February 2001

58. Net-Centric Checklist, v2.1.3, OSD NII/DCIO, 12 May 2004: http://www.defenselink.mil/nii/org/cio/doc/NetCentric_Checklist_v2-1-3_May12.docNet-Centric Operations and Warfare Reference Model (NCOW RM), DoD CIO, v1.0, December 2003,: http://in.disa.mil/
59. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised), David S. Alberts, John J. Garstka and Frederick P. Stein, CCRP, August 1999
60. Newton’s Telecom Dictionary (16th Edition), Harry Newton, 2000
61. NSTISSI No. 4009, National Security Telecommunications Information Systems Security Instruction, National Information Systems Security Glossary, September 2000
62. ONI-1573-001-00, “Worldwide: Threats to Network Centric Warfare,” October 1999 (S/NF)
63. 2000 JWSTP (Joint Warfighting Science and Technology Plan)

Appendix D Acronyms

Note: Acronyms listed in this appendix are for the purposes of this MA ICD only. Other meanings may exist.

ACRONYM	DEFINITION
ABIS	Advanced Battlespace Information System
ACTD	Advanced Concept Technology Demonstration
ALSA	Air, Land, Sea Application
AOR	area of responsibility
ASD	Assistant Secretary of Defense
AT&L	Acquisition, Technology and Logistics
ATM	Asynchronous Transfer Mode
BADD	Battlefield Awareness & Data Dissemination
BC2A	Bosnia Command & Control Augmentation
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
CDD	Capability Development Document
C&C	Computing and Communications
CDP	commander's dissemination policy
CINC	Commander in Chief
CIO	Chief Information Officer
CJTF	Commander JTF
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
COCOM	Combatant Command
COE	Common Operating Environment
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	concept of operations
COP	Common Operational Picture
COTS	commercial-off-the-shelf
CPD	Capability Production Document
D&D	denial and deception
DEW	directed energy weapons
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DoD Information Technology Standards Registry
DITSCAP	DoD Information Technology Security Certification and Accreditation Process

DoD	Department of Defense
DOJ	Department of Justice
DOS	Department of State or denial of service
DRB	Defense Resources Board
DTG	date time group
EHF	Extremely High Frequency
EMP	Electromagnetic pulse
EP	Electronic protection
ES	Electronic Support
EW	electronic warfare
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FoAPS	Family of Applications, Processes, and Services
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GI&S	Geospatial Information and Services
GIG	Global Information Grid
GOTS	government-off-the-shelf
HGI	Human-GIG Interaction
HSI	Human Systems Integration
IA	Information Assurance
IBS	Integrated Broadcast Service
IC	Intelligence Community
ICD	Initial Capabilities Document
ID	identification
IDM	Information Dissemination Management
IER	Information Exchange Requirement
IM	Information Management
IMO	Intelink Management Office
INFOSEC	Information Systems Security
IO	Information Operations
IPC	Interprocess Communications
IPT	Integrated Process Team
IS	Information Superiority
ISP	Information Support Plan
IT	Information Technology
ITW/AA	Integrated Tactical Warning and Attack Assessment
I&W	indications and warning
JITC	Joint Interoperability Test Command
JNMS	Joint Network Management System
JOA	Joint Operational Architecture
JROC	Joint Requirements Oversight Council
JTA	Joint Technical Architecture
JTF	Joint Task Force
JTRS	Joint Tactical Radio System

JTT	Joint Tactical Terminal
JV2010	Joint Vision 2010
KPP	Key Performance Parameter
MA ICD	Mission Area Initial Capability Document
MASINT	Measurements and Signature Intelligence
MILSATCOM	Military satellite communications
MIM	Mission Information Management
MLS	Multilevel Security
MNS	Mission Needs Statements
NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NBC	Nuclear Biological and Chemical
NCOW	Net Centric Operations and Warfare
NCOW-RM	Net Centric Operations and Warfare Reference Model
NGA	National Geospatial-Intelligence Agency
NIPRNET	Non-Secure Internet Protocol Router Network
NM	Network Management
NSS	National Security Systems
NTPC	Nuclear C2 Systems Technical Performance Criteria
OPCON	Operational Control
ORD	Operational Requirements Document
OSI	Open System Interconnection
QoS	quality of service
RF	radio frequency
SA	Situational Awareness
SABI	secret and below interoperability
SAR	Satellite Access Request
SATCOM	satellite communications
SCI	Sensitive Compartmented Information
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network
S/NF	Secret/No Foreign
SSI	System to System Interface
STAR	Systems Threat Assessment Report
TACON	Tactical Control
TAMD	Theater Air and Missile Defense
TBD	To Be Determined
TCP/IP	Transmission Control Protocol/Internet Protocol
TED	Threat Environment Description
TTP	Tactics, Techniques, and Procedures
USD	Under Secretary of Defense
UTA	US Imagery and Geospatial Information Service Technical Architecture
WGS	World Geodetic Survey
WMD	Weapon of Mass Destruction
XML	Extensible Markup Language

Appendix E Glossary

The following is a list of terms that will help in the development of operational requirements. The official telecommunications glossary is *Federal Standard 1037C of 1996* which can be found at: http://glossary.its.bldrdoc.gov/fs-1037/ and is maintained by the U.S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunications Sciences. Under an approved T1 standards project (LB 837), a previously developed 5800-entry, search-engine equipped, hypertext telecommunications glossary, is being updated and expanded for proposal as an American National Standard (ANS). It is currently on the Web at http://glossary.its.bldrdoc.gov/projects/telecomglossary2000. (Acronyms listed in this appendix are for GIG MA ICD purposes only; other meanings may exist.)

Access. The ability and means necessary to store data in, to retrieve data from, to communicate with, or to make use of any resource of a system (*Fed Std 1037*).

Access Control. A service feature or technique used to permit or deny use of the GIG components of a communication system (*Fed Std 1037*).

Advertise. Producer's activity of identifying and publishing information so that users become aware of products (*IDM MA ICD*).

Application. Software that performs a specific task or function, such as word processing, creation of spreadsheets, generation of graphics, facilitating electronic mail (*T1-2000*).

Architecture. (1) The design principles, physical configuration, functional organization, operational procedures, and data formats used as the bases for the design, construction, modification, and operation of a communications network. (2) The structure of an existing communications network, including the physical configuration, facilities, operational structure, operational procedures, and the data formats in use (*MIL STD 188*).

Assurance. Grounds for confidence that an information-technology (IT) product or system meets its security objectives (*T1-2000*).

Authorization. (1) The rights granted to a user to access, read, modify, insert, or delete certain data, or to execute certain programs (*Fed Std 1037C*). (2) Access rights granted to a user, program, or process (*NSTISSI 4009*).

Available Information. Information that is accessible by users through query mechanisms in accordance with their security profile and commander's priorities.

Availability. Ensures resources and data are in place, at the time and in the form needed by the user (*IA6-8510*).

Awareness. An aggregation of functional entities providing information about the available sources of data and their current contents in order to provide efficient and effective access to that data (*IDM MA ICD*).

Business Functions. DoD functions that are performed but, are not war fighting or Intelligence Community specific.

Catalog. A searchable set of metadata or indices of information products, with links to sources and locations (and possibly related metadata) (*IDM MA ICD*).

Cataloging. The process of establishing and/or maintaining a catalog (*IDM MA ICD*).

Collect. Acquiring or gathering and initial filtering of information based on a planned need, determining time sensitivity and putting the information into a form suitable for transporting.

Commander. (1) The person entitled to issue IDM policy and to exercise control over information and information system resources to effectively perform a mission (*IDM MA ICD*). (2) A person responsible for the welfare and performance of a command in accomplishing its mission. (3) Any authority whose organization defines, operates, and controls resources that participate in information processes. Commanders establish information policies, allocate resources that control those processes, and monitor their execution. (4) Any one or more personnel who are assigned and/or delegated authority, responsibility, and resources to perform a specific DoD activity.

Commander's Dissemination Policy (CDP). Expression of a set of information awareness, access, and delivery (infrastructure allocation) requirements and constraints that controls the flow of information within the commander's domain operation of IDM components and elements; issued by a commander or designee (*IDM MA ICD*).

Command Node. Any node from which a command or other organizational authority performs command activities. In the objective IDM operational context, primary command activities include (a) conducting integrated knowledge and information management activities, (b) producing integrated dissemination policies and profiles, and (c) IDM status monitoring (*IDM MA ICD*).

Common Operating Environment (COE). The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), runtime environment definitions, reference implementations, and methodology that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product (*DII COE I&RTS*).

Compilation. Information resulting from assembly of selected information elements or information requirements from multiple sources (*IDM MA ICD*).

Configuration Management. It identifies, controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational life cycle (*DoD CIO Guidance IA6-8510 IA*).

Confidentiality. Of classified or sensitive data, the degree to which the data have not been compromised; i.e., have not been made available or disclosed to unauthorized individuals, processes, or other entities (*T1-2000*).

Correlation. To put or bring into casual, complementary, parallel, or reciprocal relation. (IDM MA ICD) In intelligence usage, the process that associates and combines data on a single entity or subject from independent observation, in order to improve the reliability or creditability of the information (*JP1-02*).

Control. Control of a network resource implies an ability to monitor the resource, but also includes the ability to manipulate the functioning of that resource or to allocate it to a specific use (*DoD CIO Guidance 10-8460 NM*).

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned. (*JP1*)

Data Format. The semantics and syntax of the actual data structure. While there are many data formats in use, they may be categorized into a few basic sub-types based on the type of information they contain (e.g., textual, imagery, 3-D graphics).

Data Standardization. The process of reviewing and documenting the names, meaning, and characteristics of data elements so that all users of the data have a common, shared understanding of it.

Defense-In-Depth. The security approach whereby layers of IA solutions are used to establish an adequate IA posture. Implementation of this strategy also recognizes that, due to the highly interactive nature of the various systems and networks, IA solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured. (*DoD CIO Guidance 6-8510 IA*)

Defense Information Infrastructure (DII). The DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of DoD users across the range of military operations. It encompasses: (1) sustaining base, tactical, DoD-wide information systems, and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces to weapons systems; (2) the physical facilities used to collect, distribute, store, process and display voice, data, and video; (3) the applications and data engineering tools, methods, and processes to build and maintain the software that allow Command and Control (C2), Intelligence, Surveillance, Reconnaissance and Mission Support users to access and manipulate, organize and digest proliferating quantities of information; (4) the standards and protocols that facilitate interconnection and interoperation among networks; and (5) the people and assets which provide the integrating design, management, and operation of the DII, develop the applications and services, construct the facilities, and train others in DII capabilities and use.

Defense Information Infrastructure (DII) Common Operating Environment (COE). An application-independent basis for DoD information system architectures. The DII-COE

consists of reusable software components, a plugable framework and software infrastructure, and a set of guidelines and standards for developing, integrating, and packaging mission applications.

Level 6: Intermediate DII Compliance: Segments reuse one or more COE-component segments. Substantial security requirements are imposed upon segments at this level. Minor documented differences may exist between the User Interface Specifications for the DII and the segment's GUI implementation. Database schema, business rules, valid values, element definitions, and other features associated with a database segment are fully documented.

Level 8: Full DII Compliance: Proposed new functionality is completely integrated into the system (e.g. makes maximum possible use of COE services) and is available via the Executive Manager. The segment is fully compliant with the User Interface Specification for the DII and uses only published public APIs. The segment does not duplicate any functionality contained elsewhere in the system whether as part of the COE or as part of another mission application or database segment. The data associated with a database segment is coordinated with the Defense Data Model (DDM) and does not overlap any existing COE component database segments.

Delivery. The process by which information is transferred into a mission application destination.

Directory Services. (1) The function of providing a client with access to one or more of the sub-directories within an IDM directory and includes resolution of the network addresses used to access applications, users, and commanders. (2) Directory services provide a mechanism for accessing, distributing, and maintaining an IDM directory.

DISA COE Registry. The DoD Defense Information Systems Agency (DISA) runs an XML registry for the Defense Information Infrastructure (DII) Common Operating Environment (COE). COE is part of the DoD architecture reference model that prescribes a common set of standards for basic functions used across many applications.

Disposition. The process of deciding how to arrange or manage information by archiving, sending, or disposing of the information.

Distribution. The process of delivering information to the User.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security. (*DoD CIO Guidance IA6-8510*)

Electromagnetic Environmental Effects (E3). The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility/electromagnetic interference; electromagnetic vulnerability,

electromagnetic pulse; electromagnetic protection; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects, of lightning and p-static.

Enclave. An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN), or be based on physical location and proximity. The enclave encompasses both the network layer and the host and applications layer.

End-to-end. The inclusion of all requisite GIG components to deliver a defined capability. For the GIG, this implies all components from the user access and display devices and sensors to the various levels of networking and processing, all associated applications, and all related transport and management services. For the DISN services, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone) (*DoD CIO Guidance 10-8460 NM*).

Environment. Aggregate of procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.

External Interface. An external interface is the boundary or common point where information is exchanged between modules/entities within the GIG and those outside the GIG such as allies, coalition partners, educational institutions, governmental agencies, and other non-DoD establishments.

File. (1) The largest unit of storage structure that consists of a named collection of all occurrences in a database of records of a particular record type. (2) A set of related records treated as a unit; for example, in stock control, a file could consist of a set of invoices. (*T1 2000*)

Format. (1) The arrangement of bits or characters within a group, such as a word, message, or language. (2) The shape, size, and general makeup of a document. (*MIL STD 188*)

GIG-Enabled. Any system that exchanges and/or disseminates information in the manner described in the GIG definition, and is in compliance with the capability requirements stated in the GIG MA ICD, as appropriate and necessary to fulfill the system's operational purpose(s)/mission(s).

Global Information Grid. A DoD CIO memorandum, dated 22 September 1999 established the definition of the GIG, which subsequently was revised on 2 May 2001, by agreement among the DoD CIO, Under Secretary of Defense (USD) for Acquisition Technology and Logistics (AT&L), and the Joint Staff/J6. The GIG is defined as follows:

a. Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and

managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

b. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, and services.

c. Non GIG IT – Stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

Human-GIG Interaction (HGI). Hardware and software-enabled mechanisms and/or displays used for access and presentation of information to end users.

IDM Policy. A command statement that specifies subordinates users' awareness of and access to information, as well as precedence and priority of how that awareness and access must be achieved. IDM policies are expressed through, managed by, executed, monitored, and enforced through IDM services and tools. (*IDM MA ICD*)

IDM Profile. A user statement that delineates what information a specific user requires on an ongoing basis to execute all aspects of his assigned missions. It uses the IDM metadata schema to define its partitioning of the information. *(IDM MA ICD*)

Information. (1) The meaning that a human assigns to data by means of the known conventions used in their representation. [*JP 1-02*] (*MIL STD 188*) (2) In intelligence usage, unprocessed data of every description, which may be used in the production of intelligence. [*JP1*].

Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities (*Joint Publication 3-13 Information Operations*).

Information Delivery. (1) An aggregation of functional entities that work together to plan and manage the transfer of data to and from application entities. The functions that are used to perform information delivery are resource monitoring, policy services, profile management, and delivery planning. (2) A process by which information providers and information users apply available information infrastructure to enable the dissemination of information, in accordance with validated profiles, consistent with commanders' policies for information transfer. The process includes translation of queries and data formats (mediation), if required, to accommodate inconsistencies between source and user systems, and subordinate delivery processes at provider locations, at intermediate waypoints within the infrastructure, and at user sites. (*IDM MA ICD*)

Information Dissemination Management (IDM). A set of integrated applications, processes and services that provide the capability for producers and users to locate, retrieve, and send/receive information by the most effective and efficient means in a manner consistent with a commander's policy. The fundamental IDM services, as identified in the IDM MA ICD, are information awareness, information access, information delivery and IDM support. Through the four services, IDM provides awareness of, access to, and delivery of information across the GIG based on the priority of information flows set by the commander's dissemination policy, infrastructure availability, and security policies (joint and combined). The value of IDM increases as the access to information increases and the hierarchical relationships of information flow control are well established between the commanders within and between AORs. Additionally, the value of IDM increases as the user's specific information requirements are articulated, because the information producers can be more proactive and efficient in satisfying these requirements. IDM dependencies include robustness of the networks/communications transmission pathways, the systems on which IDM will reside, and the standardization of data, databases, and data description (metadata).

Information Exchange Requirements. Information Exchange Requirements (IERs) express the relationship across the three basic entities of an architecture (activities, elements, and information flow) with focus on the specific aspects of the information flow. IERs identify *who* exchanges *what* information with *whom*, *why* the information is necessary, and in *what manner the exchange occurs*. (*CJCSI 3170.01*)

Information Flow. (1) Any logical transportation of any form of information across a system or network. It may originate in one or more applications, be carried through any one or more network components, and end in any one or more user applications. (2) The smallest metric of traffic that is visible from the standpoint of a network's traffic routing and management capabilities. The actual implementation of an information flow is therefore highly dependent on the network type of the networks it travels across. For example, if the network uses an IP router type of network architecture, a source and destination IP address pair would define an information flow. If the network is based on an ATM network architecture, a virtual channel identifier defines information flow. The essential characteristic of the information flow in either case is that it represents the traffic aggregation that the network will base its resource allocation and traffic routing mechanisms on. All traffic within an information flow should therefore have similar network quality of service (QoS) requirements.

Information Infrastructure. The generic shareable resources (e.g., network elements, hosts, and information repositories) that are used to implement distributed information systems. More specifically, information infrastructure consists of those elements that may simultaneously provide multiple users with the services used to manipulate, store, and transfer data. All infrastructure falls into one of three sub-types: network, site, and information domain.

Information Integrity. The condition that exists when data/information is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. (T1-2000)

Information Management. The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructure.

Information Management Life Cycle. The total phases through which information is managed from creation through disposition.

Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Processes. Any activities that collect, generate, synthesize, process, exploit, store, transport, or deliver information as part of a mission operational task.

Information Producer. A person, group, or organization that creates, updates, distributes, and retires information based on their authorized/assigned missions and functions. (*DoD CIO Guidance 6-8510 IA*)

Information Product. Data organized in a variety of forms and contexts to convey intended information in relation to other data or information to contribute knowledge needed by users; it may be in the form of a data item, object, picture, document, file, database, spreadsheet, stream or other form capable of being coherently assimilated by human or machine through visual, electronic, or audible interpretation. An information product can be a file (measured by size) or a stream (measured by duration).

Information Provider. A collector or producer of information serving information users (synonymous with a "source").

Information Superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information Superiority is achieved in a noncombat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives. (*JV 2020*)

Information System. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment (hardware, firmware, and software) that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data.

Information Technology (IT). The hardware, firmware, and software used in an information system to perform information processing, transport, presentation, storage

and retrieval functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment and also includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. (*DoD CIO Guidance*)

The term "information technology", means any equipment or interconnected system or subsystem of equipment, which is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (Derived from *Title 40 US. Code, Chapter 25, Information Technology Management.*)

Information User. A person, unit, or machine (system or process) using information. (synonymous with Information Consumer.)

Infrastructure Provider(s). Functional organization(s) responsible for the wide-area, deployed, tactical, and sustaining base telecommunications and other information services among sources, commanders, and users (e.g., DISA, BNCC).

Integrate. To coherently unite elements of disparate entities to form a single new entity.

Integrity. A combined data and information system characteristic of logical correctness and reliability of the operating system, logical completeness of the hardware and software implementing the protection mechanisms, consistent data structures, and stored data.

Interface. A boundary or point common to two or more modules/entities where services are exchanged.

Interoperability. (1) Ability of information systems to communicate with each other and exchange information. (2) Conditions, achieved in varying levels, when information systems and/or their components can exchange information directly and satisfactorily among them. (3) The ability to operate software and exchange information in a heterogeneous network (i.e., one large network made up of several different local area networks). (4) Systems or programs capable of exchanging information and operating together effectively.

Knowledge. (1) Having cognizance. (2) The fact or condition of knowing something with familiarity gained through experience or association of available information. (3) The fact or condition of having information or being aware of something.

Latency. The length of the time interval between an event or stimulus and a response. In the context of IT, latency refers to the amount of time it takes from the initiation of a control to the response of a control; or from an information query to the return of information.

Metadata. Data that defines other data, an information product, such as classification, format, size, keywords, etc.

Mission Application. Any information system employed by users to produce, analyze, present, and act upon information to achieve specific mission duties. All information

flows originate and terminate in applications via their (ideally embedded) transfer systems.

Mission Category. Applicable to information systems, the mission category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD will have three mission categories:

a. Mission Critical. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified information, as well as sensitive and unclassified information).

b. Mission Support. Systems handling information that is important to the support of deployed and contingency forces. The information must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

c. Administrative. Systems handling information, which is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information). (*DoD CIO Guidance 6-8510 IA*)

Mission Profiles. Expressions of general user needs in operational terms and may draw upon a broad range of information types from a number of producer sources.

Module. A self-contained unit of a system that performs a specific task or class of tasks for supporting the major function of the system.

National Security Systems (NSS). As defined in Clinger-Cohen Act 1996, NSS includes any telecommunications or information system operated by the United States Government, the function, operation or use of which involves intelligence activities; cryptologic activities related to National Security; involves the command and control of military forces; and involves equipment that is an integral part of a weapon system. Routine administrative and business applications are not included.

Near Real Time. Pertaining to the delay introduced, by automated data processing, between the occurrence of an event and the use of the processed data, *e.g.,* for display or feedback and control purposes. *Note 1:* For example, a near-real-time display depicts an event or situation as it existed at the current time less the processing time. *Note 2:* The distinction between near real time and real time is somewhat nebulous and must be defined for the situation at hand. *Contrast with* real time. (2) Pertaining to the timeliness of data or information that has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP1)

Network. (1) An interconnection of three or more communicating entities. (2) An interconnection of usually passive electronic components that performs a specific

function (which is usually limited in scope), *e.g.,* to simulate a transmission line or to perform a mathematical function such as integration or differentiation. *Note:* A network may be part of a larger circuit. (*MIL STD 188*)

Network Centric. Exploitation of advancing technology that moves from an applications-centric to a data-centric paradigm - that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components.

Network Centric Warfare. An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

Network Management. The function of monitoring, controlling, and managing the provisioning of bearer services between two or more network elements that lie within a single common network. Network management is a sub-type of infrastructure management and is therefore a function that, while not part of IDM, must closely interact with the IDM organic functions.

Network Object. Any device, system, or application that connects to the GIG that a network manager controls. The network manager has visibility and maintains control over these objects for the Commander.

Network Operations. The organizations and procedures required to monitor, manage and control the GIG. Network operations incorporate network management, information dissemination management, and information assurance. (*DoD CIO Guidance 10-8460 NM*)

Node. In network topology, a terminal of any branch of a network or an interconnection common to two or more branches of a network. (*MIL STD 188*)

A network element that, while able to generate or receive a data stream across a network link, is not capable of providing an environment for the execution of an application. (See command node, IDM operational node, information distribution infrastructure node, producer node, user node.)

Non-repudiation. Provides the ability to prove to a third party that an entity did indeed participate in a communication. Non-repudiation is provided by the authenticating characteristics of digital signatures. (ASDIA)

Notification. The process of providing signals to Users of the immediate availability of data. By immediate, it means that the data may be delivered to the User within some period of time that the User has previously specified. The type of signal must also have been previously defined. Thus, notification services are driven, to a large extent, by a User interest profile. Notification services extend the services already available in the Web retrieval service to other information transactions such as delivery or system alerts from the metanet, transfer agent, and policy editor components.

On Demand. The user requests information based on their requirements and within the constraints of the commander's policy and the availability of the information. There are two methods for the user requesting the information. The first method is a user query for information based on the information producer's advertisement of the information availability. The second method is through the submission of a user-developed profile that requests that information be pushed on a regular user-defined schedule/preset frequency and/or pushed when available or as it has changed.

Open System. A system that implements sufficient open standards for interfaces, services, and supporting formats to enable properly engineered modules to be utilized across a wide range of systems with minimal changes, to interoperate with other modules on local and remote systems, and to interact with users in a style that facilitates portability. An open system is characterized by the following:

- well defined, widely used, preferably non-proprietary interfaces/protocols;
- use of standards which are developed/adopted by recognized standards bodies or the commercial market place;
- definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of applications; and
- explicit provision for expansion or upgrading through the incorporation of additional or higher performance elements with minimal impact on the system.

Operational Suitability. The degree to which GIG components can be satisfactorily fielded, deployed, operated, and sustained while meeting performance parameters and the users' needs.

Perception Management. Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives and objective reasoning; and to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives.

Planning Information. Planning information is used as a basis for determining future action and is generally not time sensitive. (USJFCOM White Paper - C4 to Meet the Needs of 2010 and Beyond)

Plug and Play. In a GIG context, this term implies interoperability with other GIG-enabled systems without any additional modifications or configurations required.

Policy Management. The function of overseeing the setting of, and access to, the commander's dissemination policies.

Policy Services. The aggregation of functions that support the commander and the user in the setting and usage of the commander's dissemination policy.

Prioritize. To establish a ranking system by precedence, usually to enable sharing of limited resources.

Producer. Information producers originate and supply information products in response to valid user/subscriber requirements. A producer may be a human, a system, or a process.

Producer Node. Any node where a user participates in information processes, primarily as an information producer. A producer performs the following activities: (1) receives and responds to information profiles either directly through IDM tools or through his/her C4I mission applications; (2) generates information products and standard metadata descriptions of those products, often storing them in his/her C4I repository; (3) executes information transfers in response to on-demand requests or transfer or mission profiles; (4) responds to either on-demand or profiled information searches and catalog requests; (5) monitors the IDM services to track the status of relevant activities; (6) specifies and manages information descriptor collections (catalogs).

Profile. (Synonymous with User Profile) Expression of information needs, interests, constraints, or requests (ad hoc or standing) by an information user, the user's designee, or their automated applications that enable filtering of information needed by specific users. This need is expressed independent of source but with emphasis upon timeliness required, thereby ensuring awareness of information requirements associated with mission/operation templates and consistent with applicable information policy. (1) A complete list of the information a unit must possess. (2) A detailed security description of the physical structure, equipment component, location, relationships, and general operating environments of an information system. (3) A set of parameters defining the way a device acts relative to other devices, including services required from others and provided by the device (often called a login file). (4) A profile or a combination of two types of information. First, the profile specifies a partitioning of the information space. This means that the attributes of a metadata schema can be thought of as analogous to a geospatial coordinate system and a profile, by specifying values for these attributes (e.g., file size less the 2 MB, format = JPEG), and defining regions within the information space. Any individual item of information may be located with respect to these regions (entirely inside, partially inside, entirely outside). Two key points to note are a) a single profile may specify multiple partitions (i.e., regions), and b) the "fineness" of the partitioning is limited to what may be specified by the metadata schema that is used (e.g., if the schema has the concept of nations and states but not counties, the profile will allow a distinction between information pertaining to people who live in California and those who do not, but will not allow a similar distinction between those who live in Orange County and those who do not). The second type of information contained within a profile is some sort of attribute that is to be associated with any information that falls wholly or partially within the specified partition. That attribute may be an indication of intent. By this it is meant that for each partitioning specified, an indication must be provided as to what the entity associated with the profile wants to do or intends to do, with any information that falls within that partition (e.g., delete from the local cache, queue for later delivery, replicate to a set of repositories, notify the user upon receipt). Alternatively, the attribute specified in the profile may be one of description. For example, it might be a special security compartment or an indicator of frequency of access (e.g., a profile of all data accessed less than once per week).

Profiling. The process of defining automated information dissemination criteria. Identifies information certain users require according to a specific criterion, including restrictions of the producer on authorized recipients of the information.

Quality of Service (QoS) Forecast. A prediction of the quality of service that will be available to various communities of users. A QoS forecast may, for example, indicate that BDA imagery will be transferred to all intended recipients with a predicted latency of less than 30 seconds, that weather imagery will be transferred to in-theater recipients within 20 minutes and CONUS recipients within 30 minutes, and that medical data will have a predicted latency of 15 seconds for text data and 20 minutes for image data. The function of the QoS forecast is to provide a feedback mechanism that allows the commanders to refine their policies and the operators to identify problems within the dissemination infrastructure.

Query. (1) A user request for additional or amplifying information regarding information received through some means. (2) In data communications, the process by which a master station (or mainframe or boss computer) asks a slave station to identify itself and tell its status (i.e., is it busy, alive, OK, waiting, etc.). (3) A data structure consisting of one or more search criteria and, associated with each search criteria, a set of actions. Search criteria are Boolean functions whose terms consist of metadata attributes (e.g., data of last modification, size), operators on those attributes (e.g., size <12000), or evaluation functions that operate on a data instance (e.g., key word found{China}). The set of actions associated with each search criteria indicates what the user wished to occur whenever the criteria evaluates to TRUE (e.g., retrieve the data instance, provide the user with a pointer to the data instance, provide the user with the metadata associated with the data instance, etc.).

Real Time. Pertaining to the timeliness of data or information, which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays.

Schema. Organizing structures for data; used in conjunction with a database management system or information product metadata management.

Search. To carefully and/or thoroughly peruse a domain for the purpose of finding or discovering something.

Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of information processed and stored by a computer or information system.

Security Services. The aggregation of those functions that support the creation and maintenance of information security policies and procedures.

Semantic Tag. Labeling of information based on the meaning of the content of the information and the context in which it appears.

Server. A network device that provides service to the network users by managing shared resources. *Note 1:* The term is often used in the context of a client-server architecture for a local area network (LAN). *Note 2:* Examples are a printer server and a file server (T1 2000). An information system component that provides client applications with access to a shared capability that the client does not directly support. It does so by responding to service requests from the client (it may also support service requests from other peer servers as well). A server may interact with other servers or functional entities as a result of a service request (e.g., a WWW proxy server redirects a browser's

request to another server). (NOTE: A server is not to be confused with a computer that hosts functional entities implementing the server class.) The term “server” refers solely to a function. Thus, there may be multiple computers implemented on a single server (i.e., CPU).

Smart Push. Transfer of information product(s) to information user(s) in response to profile(s) submitted (typically by the commander’s staff) in anticipation of a group of information needs. (2) The process of creating a user profile of information requirements for continuous broadcast to an operating unit or supporting entity.

Spectrum Supportability. The assurance that the necessary frequencies and bandwidth are available to military systems in order to maintain effective interoperability in the operational electromagnetic environment. It includes spectrum certification, host nation coordination, frequency assignment, and electromagnetic compatibility.

Source. (1) Organization or other entity that produces information products and, possibly, their metadata. (2) The part of a telecommunication system that transmits information. (See information producer.)

Storage. The retention of data in any form, usually for the purpose of orderly retrieval and documentation. (*JP 1-02*)

Store. Provide space for and/or maintain custody of an item for purpose of its preservation and/or to enable its future use or orderly disposal.

Subscribe. Express a standing information request (profile).

Survivability. The capability of a system to survive in a specified threat environment and accomplish its designated mission. For nuclear systems, the threat is commonly assumed to include Electromagnetic Pulse.

Survival Information. Survival information requires immediate action such as to attack the enemy, avoid being attacked, and/or to prevent fratricide. It is, therefore, extremely time sensitive. (*IDM MA ICD*)

System. The set of interrelated components consisting of mission, environment, and architecture as a whole that performs some coherent function or set of functions.

Theater Information Management. Integrated management of information within a Theater; expected to yield information flows more responsive to a CINC or similar command authority; expected specifically to integrate information management across J2, J3, J4, & J6 staff elements and functional communities.

Transfer. An activity involved in moving information from an initial location to one or more subsequent locations.

Transfer Agent. (1) An entity that interacts with source, communications, and user infrastructures to support the retrieval, transport, and delivery of information. (2) Any software module within a transfer system that supports information transfers in a manner that they may be managed by IDM services

Transfer Profile. A data structure governing the operation of a transferor.

Transport. Transport is the movement of information and/or knowledge among consumers, producers, and intermediate entities.

User. (1) Recipient of information products enabled by IDM services, governed by the recipient's profile and commander's policy. (2) A user is the ultimate consumer of all data/information. (3) A user is a human (identified through a login process) authorized to use a system. Each human will map to one user, and each user map to one human. A user is unique across the system (IDM). A user may be a human, a system, or a process.

User Node. Where a user participates in information processes primarily as an information user. A user sets information, mission, and transfer profiles, performs information searches, requests source catalogs, requests information transfers on - demand, monitors IDM to track status of information requests, and specifies and manages information descriptors collections (catalogs)

User Profile. Information characterizing an information user, facilitating the efficient data distribution of appropriate information to the user. Examples of such end user information include: allowed classification levels, user receive suite ID, times available, assigned subscriptions.

User Pull. Transfer of information product (s) to information user(s) in response to a request by and in a time frame defined by the user or their applications.

Visibility. Having the awareness of the status of a resource. It may or may not involve actually monitoring the resource. (*DoD CIO Guidance 10-8460 NM*)

Appendix F CDD/CPD to GIG MA ICD Compliance Checklist

CDD/CPDs that fall under a MA ICD must comply with any of that MA ICD's KPPs and other capability requirements as appropriate and applicable. Close examination of the CDD/CPD operational concept and information exchange requirements will help determine which KPPs/capability requirements apply. Determination of which GIG KPPs and other capability requirements are applicable to an CDD/CPD must be based on the principle that the GIG operates as a globally interconnected, end-to-end, interoperable system of systems, wherein all systems that comprise the GIG shall be GIG-enabled so as to allow "plug and play" interoperability among them. A system shall be considered GIG-enabled if it includes capabilities from the seven GIG functions described in the GIG MA ICD that are appropriate and necessary to fulfill the system's operational purpose(s)/mission(s). In order to establish whether a system is a part of the GIG, and thus subject to GIG MA ICD compliance, or not, the GIG definition should be considered very carefully (see Chapter I.A.3.a). If a system is judged to be a part of the GIG, then the next step is to determine where within the system is the origination/termination point for information to be exchanged externally with another system or systems across the enterprise (i.e. two or more systems connected or networked together end-to-end across any portion of the GIG) for the purpose of satisfying one or more information exchange requirements. In the final analysis, any system that has external information exchange requirements (or which supports and facilitates system-to-system, end-to-end flow and exchange of information, such as a transport system, network management system, etc.) must be GIG-enabled with whatever information capabilities are necessary to ensure that information exchanges can be carried out successfully and in an interoperable manner. While CJCSI 3170.01 does not specify a particular format to be used for the mandatory CDD/CPD to MA ICD crosswalk, it is recommended that the following GIG MA ICD Compliance Checklist be used to ensure that a comprehensive, complete crosswalk to the GIG MA ICD is accomplished.

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
CHAPTER I: JOINT FUNCTIONAL CONCEPT						
GIG Reference	I.B.3	Does the GIG MA ICD appear in the Related Documents section?				
GIG Implementation Guidelines	I.D	Have each of the following GIG implementation guidelines been considered and applied in the CDD/CPD as appropriate?				
		GIG implementation done in accordance with the standards included in the most current version of the *DoD JTA/DISR*?				
		All new Command, Control, Communications, Computers and Intelligence (C4I) emerging systems and upgrades to be fielded as COE/GIG ES compliant?				
		System is either standards-based or employs commercial-off-the-shelf (COTS) technologies to: • Facilitate joint, allied, and coalition interoperability? • Simplify integration? • Reduce both long and short-term costs?				
		System is to be scalable, affordable, sustainable and extensible with respect to its functionality?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
GIG Implementation Guidelines	I.D	System is designed to accommodate change and facilitate the integration of future systems and technologies as they evolve?				
		System is consistent with current DoD, IC, and commercial efforts regarding data and metadata standardization?				
		Additional manpower requirements are minimized?				
		Reliability, availability, survivability, and maintainability features of the system are designed to support all functions necessary to meet the requirements documented in Chapter IV, including the ability to recover from critical failures?				
		Emphasis is placed on reducing the complexity, time, and cost of training?				
		Software design is aimed at enhancing interoperability and commonality among GIG-enabled systems?				
		System designed using an open systems approach and adhering to applicable standards within the JTA/DISR?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
		Bandwidth and throughput requirements along with implications to strategic, fixed, theater, and tactical architectures are considered?				
		United States Imagery and Geo-spatial Information Service (USIGS) standards used for the processing and display of imagery and geospatial data across the GIG ?				
		System will be developed, tested, and deployed in a manner that is compliant with all appropriate treaties and international agreements?				
		System will be tested and certified for interoperability IAW Joint Interoperability Test Command (JITC) procedures?				
		System enables users to operate in a multilingual environment to overcome the inherent language barriers of multinational and coalition operations?				
		System mitigates security risks and meets all current security provisions articulated in appropriate DoD and IC policies, procedures, and instructions including DoD 8500.aa?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
		System uses standards-based rather than system-unique security mechanisms?				
		CDD/CPD considers ongoing developments and evolving specifications in the following areas (as applicable): • Joint Operational Architecture (JOA)? • Nuclear C2 Systems Technical Performance Criteria (NTPC)? • GIG Architecture? • Mission Information Management (MIM) Architecture?				
		Time-phased requirements developed in CDD/CPD, with associated Objectives and thresholds, IAW DoDI 5000.2?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
		Use of Standards. • Is compliance implemented IAW DoD JTA/ DISR? • Interoperability test and certification addressed as part of requirements generation process prior to production, fielding and lifecycle support IAW CJCSI 6212.01? • Technology Insertion. Applying open-system design strategies to enable insertion of new and emerging technologies while maintaining interoperability with existing GIG systems and architectures? • Data Standards. Support standardized tagging of data? • Net-Readiness. Considered NR-KPP compliance guidelines (Appendix H)?				
CHAPTER II: OPERATIONAL CONCEPT SUMMARY						
Operational Concept	II.A	If the OV-1 depicts information exchange relationships, are the producer, user, and command node entities identifiable?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
CHAPTER III: CAPABILITY GAPS						
Shortcomings	III.	Does the CDD/CPD describe shortcomings or absence of existing capabilities and systems to fulfill the needs of the GIG functions described in Chapter I? As applicable, are GIG shortcomings addressed such as: lack of interoperable applications; limited ability to rapidly catalog, search, and retrieve required information; limited ability to effectively and efficiently use existing RF spectrum; limited ability to move digital information seamlessly; lack of asset visibility resulting in limited ability to effectively manage a common user network; limited means to prioritize information and establish profiles; limited ability to support multilevel security operations?				
CHAPTER IV: REQUIRED CAPABILITIES – PROCESS FUNCTION						
Processing Efficiency and Effectiveness	IV.B.2b	All computing processes of system shall optimize the use of constrained computing and dissemination resources (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Reuse Of Information Products	IV.B.2c	System's previously generated, shareable information products (i.e., processed data) shall be reused to maximize consistency and efficiency, and to minimize process redundancy (**Threshold**)?				
Processing Mode	IV.B.2d	System shall have processes to accommodate an interactive and multimedia processing environment (**Threshold**)? System's need for processing modes other than interactive and multimedia, especially batch processing, shall be clearly demonstrated and justified prior to their adoption (**Threshold**)? System shall use time-critical processing when dealing with survival information, in order to meet stringent timeliness requirements (**Threshold**)?				
Cohesiveness	IV.B.2e	Each process of the system shall accomplish a well-defined single function so as to achieve cohesion and enhance process reusability and system maintainability (**Threshold**)?				
Modularity	IV.B.2f	System's processes shall be modular to reduce maintenance and promote reusability (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Process Reusability	IV.B.2g	System shall have, to the maximum extent possible, processes that are designed (using off–the–shelf standard components built according to an open standard) and implemented to be reusable in multiple systems and computing environments as plug and play "commodities" or "generics" rather than custom built from scratch each time (**Threshold**)?				
Reliability	IV.B.2h	System shall have processes that are classified either as deterministic or non-deterministic, with each deterministic process producing consistent and definite results, and each non-deterministic process specifying a range with boundary limits and the expected average for each output generated (**Threshold**)?				
Validation	IV.B.2i	The accuracy of outputs from the system's processes, deterministic or otherwise, shall be testable, meaning that processes shall be executable and the actual outputs generated by a process shall conform to expected outputs governed by operational requirements (**Threshold**)? In the case of the system's non-deterministic processes, it shall be possible to predict all outputs within specified limits (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Verifiability	IV.B.2j	System shall have processes that facilitate verification, and verification activities shall be performed to discover design errors and demonstrate the conformance of the system to the specified requirements (**Threshold**)?				
Interprocess Communications	IV.B.2k	To achieve interoperability among the system's processes, all processes shall use standardized mechanisms to communicate with each other, and process interfaces shall follow established standards for interprocess communications regardless of whether they are communicating with processes residing within the same computing system or with processes residing on remote systems (**Threshold**)?				
Process Prioritization	IV.B.2l	System's processes shall be responsive to task prioritization dynamically (**Threshold**)?				
Process Adaptability	IV.B2m	All critical processes of the system shall have the capability to monitor the available resources and dynamically adjust their processing characteristics and behavior in accordance with the resources made available for their use (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Standards-Based Processing	IV.B.2n	All processes of the system shall demonstrate compliance with existing directives, instructions, and prescribed standards, to include appropriate performance-based standards (**Threshold**)?				
Process Security	IV.B.2o	All processes of the system shall be protected and secured at appropriate levels and be visible to and cooperate with all information assurance operations (**Threshold**)?				
Non-GIG Interoperability	IV.B.2p	System's processing shall accommodate non-DoD (**Threshold**) and allied and coalition (**Objective**) operations when necessary?				
Robust & Flexible Processing	IV.B.2q	All process failures and processing exceptions of the system shall be handled through error handling and recovery mechanisms which are consistent with threat and risk levels associated with the processing task (**Threshold**)?				
Analytical and Collaboration Services	IV.B.2r	System's processing shall support analytical and collaboration capabilities through services that support collaborative planning, decision-making aids, modeling and simulation, data mining, intelligent agents and virtual workspaces (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Information Management Support	IV.B.2s	System's processing shall accommodate all Information Management (IM) tasks related to creation, acquisition, transmission, organization, storage, dissemination, presentation, protection and disposition of information, as well as other information processing tasks guided by and in compliance with the DoD CIO IM Strategic Plan (**Threshold**)?				
Interface Definition	IV.B.2t	All process interfaces of the system shall be well defined and clearly specified to include at a minimum all input specifications, output specifications, and specifications for controls required for triggering the process (**Threshold**)?				
Cross-Platform Functionality	IV.B.2u	System's processes shall be independent of the computing platform regardless of the programming or scripting (**Threshold**)?				
Process Availability	IV.B.2v	System's processing components shall ensure that the overall system availability is not compromised due to run-time process failures (**Threshold**)?				

CHAPTER IV: REQUIRED CAPABILITIES – STORE FUNCTION

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Data Interoperability	IV.B.3b	System shall identify and use common standards for data and metadata representation (**Threshold**)? All of a system's data that will be exchanged, or has the potential to be exchanged, shall be tagged in accordance with the JTA/DISR standard for tagged data items (e.g., Extensible Markup Language [XML], the current JTA/DISR standard), and tags shall be registered in accordance with the DoD XML Registry and Clearinghouse policy and implementation plan (**Threshold**, **KPP**)?				
Information Integrity	IV.B.3c	System's storage process shall not alter stored data in a manner that compromises the integrity of the data/information (**Threshold**)?				
Infrastructure Management	IV.B.3d	System shall provide visibility of storage infrastructure to efficiently manage storage capacity and provide the capability to remove/discard stored data as required (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Data Distribution	IV.B.3e	System's data shall be stored in a manner that facilitates distribution IAW processing and transport needs and supports the rapid retrieval of information by the user (**Threshold**)? Each item of stored data in the system shall have a single discrete source of reference so that future updates of that data, while being stored in other locations, will be able to refer back to the single reference source, thus ensuring that the information is being updated with the most current available version (**Threshold**)?				
Data Survivability	IV.B.3f	System's data shall be stored in a manner that assures the required access to and use of all needed data, and in a way that prevents the loss of stored data from physical threats such as fire, water damage, information operation threats, and Electromagnetic Pulse (EMP) as appropriate to the information being stored (**Threshold**)?				
Data Security	IV.B.3g	System's data being stored shall include its classification and releasability criteria within the semantic tag or associated schema (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Data Disposal	IV.B.3h	System's data that is no longer required shall be disposed of effectively and efficiently, so that the storage space that was used by the disposed data can be used for the storage of new data without the user having to do any additional actions once the decision to dispose has been made (**Threshold**)?				
Data Retention	IV.B.3i	System's data shall be retained in a manner that meets all mission and regulatory guidance and is transparent to the user (**Threshold**)?				
CHAPTER IV: REQUIRED CAPABILITIES – TRANSPORT FUNCTION						
Switching/ Routing/ Transmission	IV.B.4b	System providing switching, routing, and transmission control capabilities/mechanisms shall be fully interoperable and work seamlessly across the entire GIG in accordance with *DoD JTA/DISR* (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Spectrum Supportability/ Electromagnetic Environmental Effects	IV.B.4c	System shall optimize use of the available electromagnetic spectrum through efficient frequency reuse and advanced modulation, compression and filtering techniques, and shall comply with DoD, National and International spectrum management policies as applicable (**Threshold**)? System shall be mutually compatible with other systems, including allied and coalition systems, in the operational environment and shall not be degraded by electromagnetic environmental effects (**Objective**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Quality of Service	IV.B.4d	Transport system shall provide QoS capabilities that ensure that information identified as priority is delivered ahead of regular traffic 99% of the time (**Threshold**, **KPP**) and 99.9% of the time (**Objective**, **KPP**)? Required QoS factors include: Prioritization. End users shall be able to assign priority to information targeted for transport (**Threshold**)? Response Time. All transport capabilities shall be designed to meet or exceed customer stated response times (**Threshold**)? Precedence. Data shall receive expedited handling during transport in accordance with the commander's policy and user assigned priority (**Threshold**)? Reliability. Delivery of information shall be guaranteed in accordance with its assigned broadcast level (**Threshold**)? Latency. It shall be possible to deliver information in real and/or near real time as required (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Information Integrity	IV.B.4e	System shall maintain and guarantee during transport the integrity of all information elements exchanged throughout the GIG to enable user confidence; information integrity shall be 99.99% (**Threshold**, **KPP**) and 99.999% (**Objective**, **KPP**)?				
Standards	IV.B.4f	To ensure system interoperability across the GIG and to support uninterrupted service, all GIG transport capabilities shall be standards-based using *DoD JTA/DISR* and DoD CIO prescribed standards, as applicable (**Threshold**)?				
Connectivity	IV.B.4g	Transport system shall provide connectivity on demand to all fixed and deployed locations/users (**Threshold**)? Transport systems shall have the ability to maintain network connectivity on-the-move to meet Service/JTF requirements in all warfighting environments (afloat, sub-surface, airborne, in space, on the ground) (**Objective**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Capacity	IV.B.4h	With minimal exceptions, GIG transport capacity shall be viewed as an open system that is available to transport information from all domains utilizing unicast, multicast, and broadcast techniques to provide information on demand to the warfighter/decision maker (**Threshold**)? Transport system shall have the reserve capacity to accommodate surge loading and support multiple military operations as described in Defense Planning Guidance (**Objective**)?				
Technology Insertion	IV.B.4i	To effectively keep pace with advances in technology that have the potential to render existing systems obsolete shortly following acquisition, the GIG shall enable and support the seamless and efficient insertion and incorporation of emerging (future) technologies into the transport domain (**Threshold**)?				
Security	IV.B.4j	System shall provide link and transmission security based on the level of risk acceptable to the user, and the GIG security architecture shall support use of clear headers if and when necessary (**Threshold**)?				
Robustness	IV.B.4k	To avoid any single point of failure, the GIG shall use multiple connectivity paths (not susceptible to the same threat) and media (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Scalability	IV.B.4l	Transport capability shall be scalable and adaptable to meet dynamic needs of users (**Threshold**)?				
Survivability	IV.B.4m	Transport system shall be protected against all potential threats commensurate with the operating environment and the criticality of the information being transported, and shall also ensure connectivity through the total threat environment (i.e. conventional and nuclear) (**Threshold**)?				
Availability/ Reliability	IV.B.4n	Transport capabilities shall be available to provide reliable information exchange services to the warfighter/decision maker on demand and shall be responsive to the criticality of the information to be exchanged (**Threshold**)?				
Tactical Deployability	IV.B.4o	Transport system supporting tactical forces shall minimize lift requirements and be transportable using existing JTF/Service notional lift capability (**Threshold**)?				
Transport Element Status	IV.B.4p	All transport elements (e.g., switches, routers, etc.) shall be capable of providing status changes to network management devices by means of an automated capability in near real time 99% (**Threshold**, **KPP**) and 99.9% (**Objective KPP**) of the time?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Secure Voice Interoperability	IV.B.4q	Strategic and tactical secure voice systems shall be interoperable, with a 99% (**Threshold**, **KPP**) and 99.9% (**Objective**, **KPP**) call throughput success rate?				
Secure Voice with Allied and Coalition Forces	IV.B.4r	Secure voice cryptography shall be provided to or developed with allied forces that enable interoperability (**Threshold**)? Secure voice systems shall be interoperable with coalition forces (**Objective**)? A secure voice system shall be able to be provided to coalition forces that is interoperable with the U.S. version using coalition releasable technology (**Threshold**)?				
Information Over Tactical Data Links	IV.B.4s	Systems transporting/exchanging information over tactical data links (TDLs) shall use one or more members of the J-Series Family of Tactical Data Links in accordance with the DoD Joint Tactical Data Link Management Plan (JTDLMP) and the DoD Joint Technical Architecture (JTA/DISR) (**Threshold**)?				
CHAPTER IV: REQUIRED CAPABILITIES – HUMAN-GIG INTERACTION (HGI) FUNCTION						
Output/Input	IV.B.5b	System's HGI shall present to and accept information from humans using a combination of visual, aural, tactile, and/or other sensory methods (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Feedback	IV.B.5c	System's HGI shall provide unobtrusive confirmations of user input and actions, to include implicit visual, aural and/or tactile feedback in response to user actions, as well as, explicit notifications that entered data was properly entered and accepted by the system, and/or errors were detected (**Threshold**)?				
Specialized Environments	IV.B.5d	System's HGI shall functionally accommodate use in a nuclear, biological, and chemical (NBC) or other specialized operating environment as designated by mission needs (**Threshold**)?				
Usability	IV.B.5e	System's HGI shall be useable by all end user skill levels in the aspects of learnability, flexibility, and tailorability, which shall be verified by iterative user testing (**Threshold**)?				
Task Efficiency	IV.B.5f	System's HGI shall provide decision aids and tools as necessary to maximize users' efficiency and performance of their task, with operator aids designed to support specific user tasks and tailored to the information needs of the targeted user (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
User-Centered Design	IV.B.5g	A user-centered design process and user testing shall be employed for the system's HGI to ensure that the end-user's cognitive framework and expectations are accommodated by the system design (**Threshold**)?				
Standards	IV.B.5h	System's HGI shall be compliant with the DoD JTA/DISR(**Threshold**)?				
Neutrality	IV.B.5i	System's HGI presentation format shall not change the intended meaning of the information being presented; thus all data shall be clearly labeled to avoid misinterpretation or confusion (**Threshold**)?				
Ergonomics	IV.B.5j	To minimize user fatigue and discomfort, the system's HGI hardware and software elements shall be ergonomically designed with respect to the user's operating environment (**Objective**)?				
Errors	IV.B.5k	System's HGI shall be designed to minimize user input/mechanical/perception errors (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
On-line help	IV.B.5l	System's HGI shall provide context-sensitive on-line help at the user's request, thus eliminating/reducing the need for off-line support or documentation that may distract the user from the intended task (**Threshold**)?				
CHAPTER IV: CAPABILITIES REQUIRED – NETWORK MANAGEMENT (NM) FUNCTION						
Situational Gig End to End Awareness	IV.B.6.a .(2)	To accomplish GIG end-to-end situational awareness, system shall have the NM capability of automatically generating and providing an integrated/correlated presentation of network and all associated network assets (**Threshold**)?				
Dynamic, Predictive Planning	IV.B.6.a . (3)	System shall have the NM capability to perform dynamic, predictive planning by gathering, storing and using knowledge about GIG assets/resources, so as to optimize their utilization (**Threshold**)? System shall have the NM capability to create/modify/distribute network plans and orders IAW user requirements (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Distributed and Partitioned Network Control	IV.B.6.a. (4)	System shall have the NM capability to rapidly transfer control of one or more objects or groups of varying size, and reestablish control when relinquished without hindering end-to-end visibility by the senior network manager, while maintaining continuous control (**Threshold**)?				
Remote Object and Network, Control and Configuration	IV.B.6.a. (5)	System shall have a NM capability that leverages existing and evolving technologies and has the ability to perform remote network device configuration/reconfiguration of objects that have existing DoD JTA/DISR management capabilities (**Threshold**)?				
Network Status	IV.B.6.a. (6)	System shall have an automated NM capability to obtain the status of networks and associated assets in near real time 99% (**Threshold**, **KPP**) and 99.9% (**Objective**, **KPP**) of the time?				
Automated Fault Management	IV.B.6.a. (7)	Systems shall have the NM capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving (**Threshold**)?				
CHAPTER IV: REQUIRED CAPABILITIES – INFORMATION DISSEMINATION MANAGEMENT (IDM) FUNCTION						

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Requirement Identification	IV.B.6.b. (2)	System shall have an IDM capability to assist users in efficiently identifying their information requirements in a manner that captures key attributes associated with these requirements (e.g., timeliness, quantity, confidence level, etc.) (**Threshold**)?				
Search Driven Information	IV.B.6.b. (3)	System shall have an IDM capability to acquire needed information by search queries, with successful searches yielding 85% of available, needed information based on the user query and with no more than 20% of the received information being irrelevant/unusable (waste) or failed searches (**Threshold**, **KPP**); and yielding 95% of available, needed information and with no more than 10% of the received information being irrelevant/unusable (waste) or failed searches (**Objective**, **KPP**)? System shall have an IDM capability to locate and characterize available information of interest that minimizes information overload (**Threshold**)?				
Information Advertisement	IV.B.6.b. (4)	System shall have an IDM capability through which an information producer's products become known to the user population (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Quality of Advertisements	IV.B.6.b. (5)	System shall have an IDM capability that will enable information producers to describe their information products accurately using established search wCDD/CPDs and level of description 90% of the time (**Threshold**)?				
Product Descriptions	IV.B.6.b. (6)	System shall have an IDM capability that enables information producers to label their products using standardized metadata (including classification) (**Threshold**)?				
Source Cataloging	IV.B.6.b. (7)	System shall have an IDM capability that enables information producers to automatically build catalogs of information products and product updates based on available information products and users' profile requests (**Objective**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Profile Management	IV.B.6. b. (8)	System shall have an IDM capability that supports building profiles based on collaboration of information requests from users (through their profile requests), the commander's IM policy, and on information producers applying appropriate rule sets (e.g. security) (**Threshold**)? System shall have an IDM capability that enables profiles to be transferable and reusable (**Threshold**)? System shall have an IDM capability that enables automatic recognition of a change in Commander's Dissemination Policy (CDP) during profile creation, alerting the customer to that change and adjusting/modifying the profile to conform to the CDP (**Threshold**)?				
Profile Driven Information	IV.B.6.b. (9)	System shall have an IDM capability that enables the user to identify information requirements (**Threshold**)? System shall have an IDM capability that, once a profile is posted, enables information producers to automatically disseminate a minimum of 95% of available, needed information, with no more than 15% of the information received being irrelevant/unusable (waste) (**Threshold**); and a minimum of 99% of available, needed information, with no more than 10% of the information received being irrelevant/unusable (waste) (**Objective**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Filtering of Multiple Sources	IV.B.6.b. (10)	System shall have an IDM capability that provides a means to filter out superfluous information to the level of fidelity as determined by the local commander (**Threshold**)?				
Geographic Areas	IV.B.6.b. (11)	System shall have an IDM capability that enables information producers to disseminate information to a specific geographic area and to the users who are within that area (**Threshold**)?				
Commander's Dissemination Policy Generation	IV.B.6.b. (12)	System shall have an IDM capability that provides a means for assisting commanders in rapidly building effective and intuitive information dissemination policies and to automate readjustment of subordinate commands' dissemination policies with appropriate alerts to those commands that policy has changed (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Information Flow Awareness	IV.B.6.b. (13)	System shall have an IDM capability through which commanders become aware of the information flowing within their AOR to facilitate adjustments to meet operational mission requirements (**Threshold**)? System shall have an IDM capability for monitoring and tracking information flows to identify trends; for forecasting volume, content, and quality of service consistent with information and mission requirements; and for predicting the results of information control policies to optimize available resources consistent with mission priorities (**Objective**)?				
Allied Access	IV.B.6.b. (14)	System shall have an IDM capability that supports US/allied (**Threshold**)/coalition (**Objective**) accessibility to information, conforming to a commander's dissemination policy and DoD and IC security regulations?				
Status	IV.B.6.b. (15)	System shall have an IDM capability to track and report the status of the satisfaction of information requirements from the point of information request to delivery of requested information (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Resource Monitor	IV.B.6.b. (16)	System shall have capability to monitor and control IDM core services and distribute system status information to IDM administrators (**Threshold**)?				
Controlled Access	IV.B.6.b. (17)	System shall have an IDM capability to regulate access to information in accordance with information assurance policies and procedures, and a commander's dissemination policy, to include the ability to constrain/control the awareness of the existence of information (**Threshold**)?				
Information Description	IV.B.6.b. (18)	System shall have an IDM capability to access information from the GIG using standard metadata (**Threshold**)?				
Delivery Plan	IV.B.6.b. (19)	System shall have an IDM capability to build an end-to-end delivery plan based on user information requirements, mission priorities, dissemination policy, and available transport resources (**Threshold**)? System shall have an IDM capability to dynamically adjust delivery plans based on changes to user information requirements, mission priorities, dissemination policy, and available transport resources (**Objective**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Information Retrieval	IV.B.6.b. (20)	System shall have an IDM capability to retrieve information of interest that has been located (**Threshold**)?				
Collection Request	IV.B.6.b. (21)	Systems shall have an IDM capability to request the collection and production of information that is required by a user but that is not already available (**Threshold**)?				
Dynamic Profiling	IV.B.6.b. (22)	System shall have an IDM capability to activate/deactivate information requirements based on external influences such as mission, role, time, location, situation, and environment (**Threshold**)?				
Delivery Management	IV.B.6.b. (23)	System shall have an IDM capability to assign attributes (e.g., priority, QoS) to information that will govern its dissemination and also provide a means to convey the attributes (e.g., priority, QoS, etc.) of information to the transport system (**Threshold**)? System shall have an IDM capability to assign precedence for information, which will govern its dissemination throughout the GIG, and shall ensure that the priority for an information requirement shall be carried with all the elements of information required to satisfy that information requirement, to include the ability to apply precedence to blocks of information packets for digital voice service to ensure QoS (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Policy Management	IV.B.6.b. (24)	System shall have an IDM capability for commanders, and those delegated information flow authority within an organization, to dynamically adjust their information dissemination policies (**Threshold**)?				
Survival Information Dissemination	IV.B.6.b. (25)	Systems shall have an IDM capability that, utilizing a standard schema, IAW the commanders' dissemination policies and user profiles, will support the means for prioritization of information flows within a theater, using theater apportioned resources, and enable dissemination of survival information (limiting survival information to less than 12 kb) within the time frames of the matrix portrayed in Figure 5, 95% of the time (**Threshold**, **KPP**) and 0.5 seconds 95% of the time (**Objective**, **KPP**)?				
Correlation	IV.B.6.b. (26)	System shall have an IDM capability to minimize the delivery of redundant information as well as the capability to identify complimentary, parallel or reciprocal relationships among information elements (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Notification	IV.B.6.b. (27)	System shall have IDM capabilities (**Threshold**) for notification of: • changes in policy? • changes in user information requirements? • information becoming available or changing? • changes in network status? • changes in provider and user system status? • the delivery/receipt of information? • status of IDM services? • product availability? • a conflict within the delivery plan? System shall have an IDM capability that gives the user the option of being notified when information related to his/her requirements becomes available or when changes occur; in the case of survival information, notification will be automatic (**Threshold**)?				
Flexibility	IV.B.6.b. (28)	System shall have IDM capabilities that can be applied from the strategic to the tactical levels without major software modifications (**Threshold**)?				
Scalability	IV.B.6.b. (29)	System shall have IDM capabilities that are scalable to meet system and operational user requirements (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Directory Services	IV.B.6.b. (30)	System shall have an IDM capability that provides directory services with minimal personal intervention (**Threshold**)?				
CHAPTER IV: REQUIRED CAPABILITIES – INFORMATION ASSURANCE (IA) FUNCTION						
Information Integrity and Availability	IV.B.6.c. (2)	System shall be robust, survivable and capable of rapid restoration, to support IA across the GIG (**Threshold**)? System shall have an IA capability to define, control, and defend enclave boundaries (**Threshold**)? System shall have an IA capability to provide timely, reliable access to processes and data even in the event of a denial of service attack (**Threshold**)? System shall have an IA capability to ensure information and process integrity throughout the system (during storage, processing, transmission and presentation) to prevent unauthorized or unintended changes, in accordance with mission specific criteria (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Prevent Opportunity to Attack	IV.B.6.c. (3)	System shall be developed in accordance with IA Defense in Depth standards (CJCSI 6510.01C) to prevent or at least minimize the opportunity for attack; and shall have, in the event of an attack, the IA capability to immediately define, detect and respond appropriately to anomalies/attacks/disruptions from external threats, internal threats and natural causes (**Threshold**)?				
Access Control	IV.B.6.c. (4)	System shall have an IA capability that provides adequate protection from user attempts to circumvent system access controls, accountability or procedures for the purpose of performing unauthorized system operations (**Threshold**)?				
Detection and Responses	IV.B.6.c. (5)	System shall incorporate a detection, reporting and response IA infrastructure that enables rapid detection of and reaction to anomalous events, and enables operational situation awareness and responses (**Threshold**)?				
Security Domains	IV.B.6.c. (6)	System shall have an IA capability for operating within each security domain and across any security domains while ensuring that all operations are comply with existing security requirements (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Authentication/ Confidentiality/ Non-repudiation	IV.B.6.c. (7)	System shall meet and maintain minimum IA Defense in Depth standards, including certification and accreditation IAW DITSCAP process (e.g., *CJCSI 6510.01C*, *DoDI 5200.40*) (**Threshold**/**Objective**, **KPP**)? System shall utilize/interoperate with the security management infrastructure (e.g., key management and DoD public key infrastructure) (**Threshold**)? System shall provide proof of information origin and receipt as required (**Threshold**)?				
Confidentiality Services	IV.B.6.c. (8)	System shall have an IA capability that ensures information is not disclosed to unauthorized entities or processes on the network and infrastructure so as to protect against passive intercept attacks, including against unauthorized disclosure of information and traffic analysis (**Threshold**)? System shall have an IA capability to share data among users operating at different and /or multiple security levels as appropriate, and at the same time protect the data from unauthorized disclosure (**Threshold**)?				

GIG MA ICD COMPLIANCE CHECKLIST						
MA ICD Section Heading	**MA ICD Para #**	**CROSSWALK ITEMS**	**CDD /CPD Page**	**CDD/ CPD Para**	**CDD/ CPD Line #**	**YES, NO, N/A**
Content-Based Encryption	IV.B.6.c. (9)	System shall have an IA capability to perform content-based encryption of information objects at the host instead of depending on the bulk encryption of the entire network in order to secure the information (**Threshold**), and this capability shall also be available for operations involving allied and coalition forces (**Objective**)?				
CHAPTER IV: REQUIRED CAPABILITIES – INTEROPERABILITY						
Interoperability	IV.C	System shall satisfy all critical IER attributes to the Threshold level (**Threshold**, **KPP**) and satisfy all IER attributes to the Objective level (**Objective**, **KPP**)? Refer to note at the end of paragraph IV.C concerning the transition from I-KPP to the NR-KPP.				
CHAPTER V: OPERATIONAL ENVIRONMENT-THREAT						
Threat to be Countered	V.A	If information exchange is fundamental to the CDD/CPD, does Chapter IV mention Information Operations, Computer Network Attack, Computer Network Exploitation, Electronic Warfare, and Electromagnetic Pulse?				

Appendix G GIG Information Exchange Requirements (IERs)

1. The GIG diagram in Figure 6 illustrates information exchange requirements for the GIG (OV-3). These information exchanges become the foundation for a more complex architecture that will form the basis for detailed information exchange requirements in ORDs/CDDs. Note that the diagram is intended to represent logical interactions and information flows, not physical connectivity.

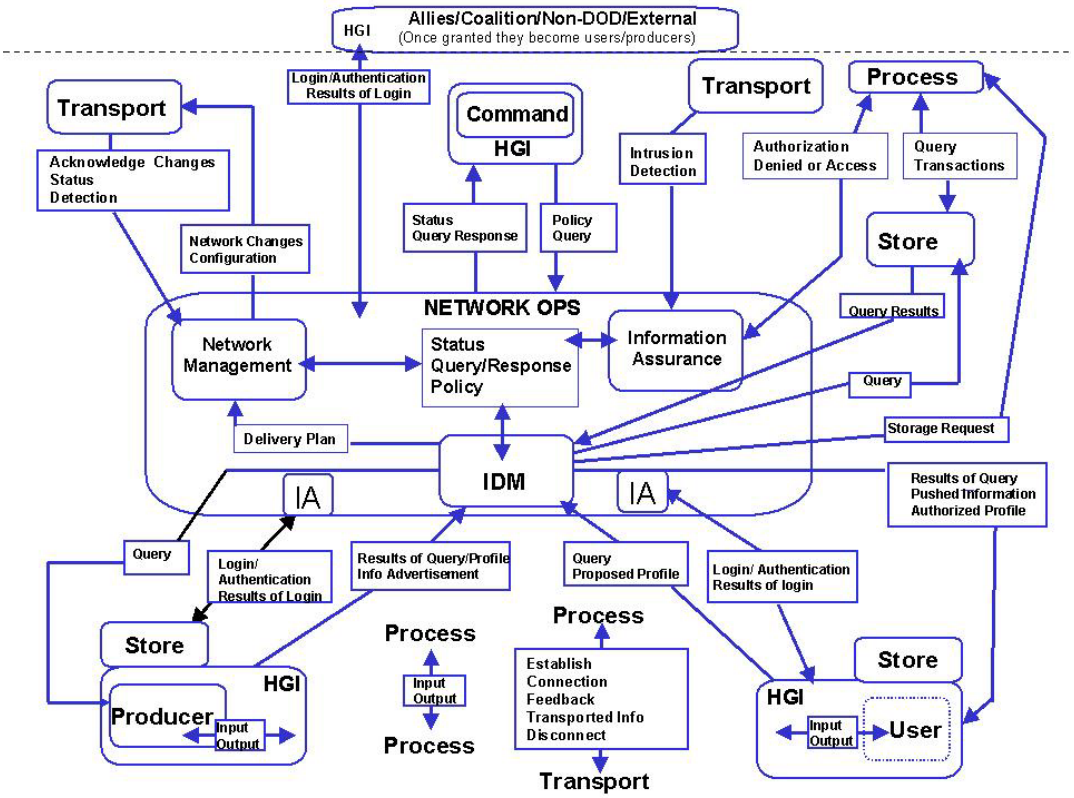


Figure 6. GIG IERs

2. The following paragraphs describe the major elements of the GIG IERs:

   a. Command Node. An entity, internal to the GIG that is organized to gather, process, analyze, display, and disseminate planning and operational data and perform other related tasks. In the **Objective** GIG operational context, the primary command activities include:

      - Conducting integrated knowledge and information management activities
      - Producing integrated dissemination policies and profile guidance
      - Monitoring GIG status and information flows

   b. Information User. A user is an entity internal to the GIG that participates primarily as a consumer of information. A user:

      - Proposes information profiles
      - Performs information searches

- Receives profiled information
- Monitors status of information requests
- Can store or dispose of information

c. Information Producer. A producer is an entity internal to the GIG that creates, updates, distributes, and retires information based on authorized/assigned missions and functions.. A producer:
   - Receives and responds to information profiles
   - Generates information products and standard metadata descriptions of those products
   - Executes information transfers in response to on-demand requests or standing profiles
   - Monitors GIG services to track the status of relevant activities

d. Allies/Coalition/Non-DoD/and other Entities External to the GIG. These entities are external users/producers who require access to the GIG. Once access is granted, they become users/producers as required. The NETOPS Node receives the access IER so that IA, NM, and IDM can coordinate the security access, physical connection and dissemination considerations that must be made. NETOPS is receiving its external policy procedures from the command node. This node includes NSC, DOS, DOJ, FEMA, etc.

e. The remainder of the nodes are the functional/logical entities of the GIG described in Chapters I and IV. It should be noted that these functional entities also act as senders and/or receivers of information and will exchange information with other like nodes. For example NM to NM will exchange status information, Transport to Transport will handshake, and Store to Store will perform remote retrieval.

   Note: The terms "Information User" and "Information Producer" and “Command” depend on the activities being performed by an entity. Producers can also be users and vice versa. Due to the complexity of Figure 6, all requisite mechanisms for protecting security domains and enabling multilevel secure information flows and fusion are not explicitly shown.

3. Applicability to CDDs/CPDs/MA ICDs. The information exchange requirements depicted in Figure 6 represent the high-level exchange requirements that can apply to any system. Any IER found in a non-IT CDD/CPD/MA ICD will always contain a sending node and receiving node, which corresponds to the user, and producer node in the GIG IER diagram. Although more specific in nature, the Event and Information Characterization columns will always contain one of the basic elements of user/producer exchange such as query, status, results of query, pushed profile information, and information advertisements. Optional fields that should be considered are: timeliness, data recognition, frequency and data relevance.

4. Examples of Applicability.

Table D-1. ORD IER Extracts

Advanced Amphibious Assault Vehicle

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
TA1.1	Combat ID	PLI,SA info for surface to surface CID	AAAV(C) AAAV(P)	U.S. Armored Systems (Shooters)	Y	Survival information Dissemination

Integrated Collaborative Collection Management

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
SN 2.5	Smart Push	Send finished imagery/products to users based on pre-designated criteria.	Exploit/ Production Centers	All authorized users including allies and coalition partners	Y	Survival Information Dissemination * This IER should trigger the ORD writer to think about how the coalition requests and is granted access in their system because the GIG IERs include an external GIG access IER

Joint Tactical Radio System

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
OP 5.1.1	System Network Information and Status	System and Network Reports	JTRS NMS	JTRS NMS	N	Status from Transport and Process to Network Management

Defense Joint Accounting System

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
SN 4.7	Populate data warehouse		DPPS-DCD	DJAS	Y	Store Request

Global Combat Support System

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRIT	SUPPORTS GIG IER
Compliance Checklist contained at Appendix F.	Joint Decision Support Tools	Provide graphical displays to depict units and infrastructure Provide drill down capabilities to identify…	GCSS-A GCSS-AF GCSS-MC GCSS-M BSM JTAV JPAV GTN JOPES	NCA CINC JTF Services	Y	Request for Information

Table D-2. Sample GIG IER Matrix

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRI-TI-CAL	INFORMA-TION INTEGRITY	DATA ACCES-SIBILITY	Timeliness
SN 5 ST 5 OP 5 TA 5	Commander's Information Policy – Initial/Update	Policy	Command	IA,IDM,NM	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
SN 5 ST 5 OP 5 TA 5	Request for information	Query	Command	IA,IDM,NM	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
			User	IDM				
			IDM	Producer				
			IDM	Store				
			Process	Store				
			IA,IDM,NM	IA,IDM,NM				
SN 5 ST 5 OP 5 TA 5	Response from Receiving Node	Results Of Query	IA,IDM,NM	Command	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
			IDM	User				
			Producer	IDM				
			Store	IDM				
			Store	Process				
			IA,IDM,NM	IA,IDM,NM				
SN 5 ST 5 OP 5 TA 5	Operational Assessment of IA, NM, IDM	Status	IA,IDM.NM	Command	Y	99.99% (T) 99.999% (O)	Semantic Tag*	User-specified
	Operational Assessment of transport		Transport	NM				

UJTL	EVENT	INFO CHAR	SENDING NODE	RECEIVING NODE	CRI-TI-CAL	INFORMA-TION INTEGRITY	DATA ACCES-SIBILITY	Timeliness
	Operational Assessment		IA,IDM,NM	IA,IDM,NM				

Semantic Tag* - As Applicable

User-specified – The users' request for information based on their requirements and within the constraints of the commander's policy and the availability of the information. There are two methods for the user to request information. The first is a user query for information based on the information producer's advertisement of the information availability. The second method is through a profile that requests that information be automatically disseminated on a defined schedule and/or disseminated immediately when available or as it has changed.

Appendix H. Net-Ready Key Performance Parameter (NR-KPP) Compliance Guidelines

The degree of net-readiness that can be achieved will be determined primarily by assessment and evaluation against the following four basic components of the NR-KPP, per guidance issued in CJCSI 6212.01C, "Interoperability and Supportability of Information Technology and National Security Systems," November 20, 2003, which states that, at a minimum, the NR-KPP is comprised of the following elements:

- Compliance with the Net-Centric Operations and Warfare Reference Model (NCOW)
- Compliance with applicable GIG Key Interface Profiles (KIPs)
- Compliance with DoD Information Assurance requirements
- Supporting integrated architecture products

Specific guidance and assistance for capability document authors in understanding net-centric attributes and capabilities required to move into the net-centric environment in the Global Information Grid, and in determining and documenting NR-KPP compliance, is provided in this Appendix, which contains relevant material excerpted from Enclosures F through G of CJCSI 6212.01C; from Chapter 7 of the Defense Acquisition Guidebook, "Acquiring Information Technology and National Security Systems;" and from the OSD NII/DCIO Net-Centric Checklist. CJCSI 6211.01C is available at the following site: http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf. The latest version of the Defense Acquisition Guidebook can be found at http://dod5000.dau.mil/ and the most current version of the Net-Centric Checklist is located at the NII Document Archives site at http://www.dod.mil/nii/doc/ (a listing of Net-Centric Attributes can also be found at this site).

Guidelines from Enclosures F through G of CJCSI 6212.01C:

All CDDs and CPDs initiated on or after 21 May 2004 must include a NR-KPP statement. The NR-KPP definition statement will document that all requirements will be satisfied to the standards specified in the threshold value and objective values. Threshold value is 100 percent of interfaces; services; policy enforcement controls; and data correctness, availability and processing requirements designated as enterprise-level or critical in the Joint integrated architecture. Objective value is 100 percent of interfaces; services; policy enforcement controls; and data correctness, availability and processing requirements in the Joint integrated architecture. (Note: Data processing is defined as the input, output, verification, organization, storage, retrieval, transformation and extraction of information from data.) The NR-KPP statement alone does not ensure interoperability requirements; a system must also be designed against the appropriate architectures, most current version of the DOD JTA/DISR and IA standards.

CDD and CPD authors should refer to Net-Centric Assessment Criteria detailed in Enclosures F through G of CJCSI 6212.01C. These criteria are intended to assist program managers to characterize the net-centric attributes of their services and data products.

Guidelines from the Defense Acquisition Guidebook:

Required Documentation:

Does the capability have the following required documentation?:

- AV-1, OV-2, OV-4, OV-5, OV-6c, SV-4, SV-5, SV-6
- JTA/DISR Standards Compliance with draft TV-1
- LISI Interconnectivity Profile
- NR-KPP Compliance Statement
- NCOW-RM Compliance
- IA Compliance Statement
- KIP Declaration List

Supporting Integrated Architecture Products

- Have all architecture products been developed in accordance with the DoD Architecture Framework?
- Does the AV-1 describe a net centric environment?
- Has the TV-1 been prepared using applicable information technology standards profiles contained in the JTA/DISR?
- Have all the interfaces listed in the OV-2 and SV-6 been appropriately labeled with the GIG core enterprise services needed to meet the requirements of the applicable capability integrated architecture?
- Have all the applicable OV-5 activities identified in the specific capability integrated architecture been appropriately described at each critical or enterprise level interface in terms of policy enforcement controls and data enterprise sharing activities in the NCOW-RM, Node Tree OV-5?
- Have specific capability integrated architecture OV-6c time event parameters been correlated with GIG architecture OV-6c?
- Have verifiable performance measures and associated metrics been developed using the integrated architectures, in particular, the SV-6?

Key Interface Profiles (KIPs)

- Have applicable Key Interface Profiles definitions been included as part of the KIP compliance declaration?

- Are the information technology standards for each applicable KIP technical view included in the draft TV-1 for the specific Joint integrated architecture?
- Are the appropriate KIP test procedures addressed as part of the requirement for interoperability system testing and certification?

Net-Centric Operations and Warfare Reference Model (NCOW)

- Have the activities listed in the applicable capability integrated architecture OV-5 been mapped to the NCOW-RM node tree OV-5 activities? Recommend that applicable capability integrated architecture OV-5 activities be characterized by use case diagrams grouped under the applicable GIG Core Enterprise Services (e.g., Discovery, Messaging, Mediation, Collaboration, etc.) to meet net-centric capabilities requirements for managing net-centric information environment.
- Have NCOW-RM OV-5 activities been used to identify requirements for data correctness, data availability and data processing necessary for posting data/information elements within a specific joint integrated architecture?
- Has the SV-4 systems functionality been mapped to the applicable GIG Core Enterprise Services?
- Are the information technology standards in the NCOW-RM Target Technical View included in the Draft TV-1 for the applicable capability integrated architecture?

Information Assurance

- Have applicable information assurance requirements of DoD 8500 Series issuances and DCI Directives been identified for all GIG core enterprise services needed to meet the requirements of the specific joint integrated architecture?
- Has the applicable capability received IA certification and accreditation documentation from the appropriate Designated Approval Authority?

Guidelines from the OSD NII / DCIO Net-Centric Checklist:

The purpose of the Net-Centric Checklist is to assist program managers in understanding the net-centric attributes that their programs need to implement to move into the net-centric environment as part of a service-oriented architecture in the Global Information Grid. A service-oriented architecture is a design style for building flexible, adaptable distributed-computing environments for the Department of Defense (DoD). Service-oriented design is fundamentally about sharing and reuse of functionality across diverse applications. Service-oriented design focuses on the following best practices:

- Design application and system functionality as accessible and reusable services
- Expose service functionality through programmatic interfaces
- Maintain an abstraction layer between service interfaces and service implementations
- Describe service interfaces using standard metadata
- Advertise and discover services using standard service registries
- Communicate with services using standard protocols

Programs must address the Department of Defense's Net-Centric Data Strategy for the following:

- Ensuring that data are visible, available, and usable when needed and where needed to accelerate decision-making
- "Tagging" of all data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery of data by users
- Posting of all data to shared spaces to provide access to all users except when limited by security, policy, or regulations
- Advancing the Department from defining interoperability through point-to-point interfaces to enabling "many-to-many" exchanges typical of a network environment

To implement the Information Assurance Strategy to transition to a net-centric environment, programs must take advantage of the following:

- An integrated Identity Management, Permissions Management, and Digital Rights Management
- Ensuring that adequate confidentiality, availability, and integrity are provided

  In developing capability documents, authors should consider the following basic questions:

  Net-Centric: How is the system Net-Centric? If not, when is it programmed to be? If not programmed to be, what is the sustainment plan?

  DoD Joint Technical Architecture: Describe the IT/NSS standards that the system has implemented from the DoD Joint Technical Architecture (DoD JTA/DISR, Version 6.0). If not, when is it programmed to do so? If not, explain why they are not being used.

  DoD Net Centric Operations and Warfare Reference Model: How is the system aligned with the DoD Net-Centric Operations Warfare Reference Model? If not, when is it programmed to be aligned?

  Architecture Views: Be prepared to provide architecture view products (Operational Views [OV], System Views [SV], and Technical Views [TV]) which comply with the product definitions in the DoD Architecture Framework (DoD AF). If not, when is it programmed to have these products?

  There are four sections in the Net-Centric Checklist:

- Data
- Services
- Information Assurance/Security
- Transport

Note: The complete Net-Centric Checklist is not provided within this GIG Mission Area ICD. However, it is recommended that in order to perform the most thorough net-centricity evaluation/assessment, capability document authors should consider the full set of Checklist questions associated with each of the following capabilities/design tenets, as applicable/appropriate:

Data (DoD Net-Centric Data Strategy)

Design Tenet: Make data visible
Design Tenet: Make data accessible
Design Tenet: Make data understandable
Design Tenet: Make data trustable
Design Tenet: Make data interoperable
Design Tenet: Provide Data Management
Design Tenet: Be Responsive to User Needs

Services

Design Tenet: Service-Oriented Architecture
Design Tenet: Open Architecture
Design Tenet: Scalability
Design Tenet: Availability
Design Tenet: Accommodate heterogeneity
Design Tenet: Decentralized operations and management
Design Tenet: Enterprise Service Management

Information Assurance/Security (DoD Net-Centric IA Strategy)

Design Tenet: Net Centric IA Posture and Continuity of Operations
Design Tenet: Identify Management, Authentication and Privileges
Design Tenet: Mediate Security Assertions
Design Tenet: Cross Security Domains Exchange
Design Tenet: Encryption and HAIPE
Design Tenet: Employment of Wireless Technologies

Transport

Design Tenet: IPv6

Design Tenet: Packet Switched Infrastructure
Design Tenet: Layering, Modularity
Design Tenet: Transport Goal
Design Tenet: Network Connectivity
Design Tenet: The Concurrent Transport of information Flows
Design Tenet: Differentiated Management of Quality-of-Service
Design Tenet: Inter-Network Connectivity
Design Tenet: Joint Technical Architecture
Design Tenet: RF Acquisition
Design Tenet: Joint Net-Centric Capabilities
Design Tenet: Operations and Management of Transport and Services

Note: The Net-Centric Checklist will be updated as needed to reflect DoD standards and Industry best business practices. As standards and protocols are approved in the Joint Technical Architecture/DISR or the Net-Centric Operations and Warfare Reference Model, they will be added to the Checklist. In addition to the Net-Centric Checklist items mentioned above, a listing of Net-Centric Attributes can be found on the same OSD NII /DCIO site that contains the Checklist: http://www.dod.mil/nii/doc/

Appendix I. Acknowledgments

In late November 1999 the Joint Chiefs of Staff (JCS) Joint Requirements Oversight Council (JROC) tasked US Joint Forces Command (USJFCOM) to develop a Global Information Grid (GIG) Capstone Requirements Document (CRD) and return to the JROC for formal approval of the document. Twenty-one very interesting and challenging months later, in August 2001, USJFCOM successfully completed its task and the GIG CRD was approved. However, the creation of a document of the size, scope and far-reaching impact of the GIG CRD would be impossible without the contributions of a great many talented and dedicated people. Therefore, USJFCOM, as the Executive Agent for the GIG CRD, wishes to express its sincere thanks to all those from throughout the Department of Defense, the Intelligence Community, private Industry and elsewhere who participated during the CRD development, review and approval process and contributed in immeasurable ways. Within USJFCOM, the C4 Systems Directorate (J6) had overall management oversight for the development of this CRD, with its C4 Plans, Policy and Projects Division (J61) specifically assigned as the project lead. Two former USJFCOM J6 Directors, Brigadier General Jerry McElwee, US Army (Retired), and Brigadier General Anthony “Bud” Bell, US Air Force (Retired), and one former and one incumbent J61 Division Chief, Captain Ric Rushton, US Navy, and Captain Joe Horn, US Navy, respectively, deserve special thanks for providing the GIG CRD development team with strong and committed leadership and clear direction, and for very actively participating in the development process themselves. They all gave the team the benefit of their visionary thinking and constructive ideas on numerous occasions, especially in terms of how the document could best serve the needs of the Joint Warfighter. While not assigned as part of the core GIG CRD development team, the following individuals at USJFCOM were called into service on many occasions as “adjunct” team members and always rose to the task with significant contributions to the cause and thus warrant particular thanks: Keith Young; Wayne Richards; Kenny Williams; Lieutenant Colonel Paul Glora, USMC Reserve; Fred Prickett; Steve Vangundy; Tony Grayson; Mark Orr; Master Sergeant David Thompson, US Air Force Reserve; Lieutenant Colonel Jane Rohr, US Air Force Reserve; Brian Duval; Bruce Driscoll; Carolann Smith; Tim Ruck; Mike Slaughter; Lieutenant Colonel Jack Hoesly, US Army; Major Andre Washington, US Army; Major Robert Logsdon, US Army; John Dorris; Tom Lang; Dave Vanderford; Joe Gisler; Dave O'Neill; Colonel George Bowers, US Army; Captain Alex Urrutia, US Navy; Lt Col Kristine Clifton, US Air Force; MSgt Matthew Fischer, US Air Force; Lieutenant Steven Eisenhauer, US Navy; Lt Col Terry Boston, US Marine Corps; Ray Crouch; Steven Derganc; Mark Klett; Commander Bill Mosk, US Navy; Lieutenant Vincent Augelli, US Navy; Bob Banford, Stephanie Yoder; Ed Wied; David Shaw; Lieutenant Commander Pat Bindl, US Navy; Eddie Nikolas; and Wendy Richardson. And that brings us finally to the GIG CRD development team itself, a very small core group of incredibly talented, creative, dedicated and productive individuals who took on a daunting task, overcame every

obstacle in the way and in the end produced a very high quality document that will have a positive impact on the Department of Defense and the Intelligence Community well into the future. USJFCOM offers its deepest and most sincere gratitude to its GIG CRD "all stars" Art Macdougall, Dr. Mukesh Rohatgi, Duncan Bell, and Laurie Redmond for a job extremely well done! Each of you is also to be especially commended for helping Lieutenant Colonel Terry Mansfield, US Army, Project Manager and Principal Author and Editor of the GIG CRD, close out his twenty-three year military career on a very high note, and for affording him the privilege and honor of serving proudly with you all.